

Regulation of Cross-Border Transfers of Personal Data in Asia (ABLI Legal Convergence Series)

Asian Business Law Institute



ABLI Legal Convergence Series

REGULATION OF CROSS-BORDER TRANSFERS OF PERSONAL DATA IN ASIA



ASIAN BUSINESS LAW INSTITUTE

ABLI Legal Convergence Series

**REGULATION
OF
CROSS-BORDER TRANSFERS
OF
PERSONAL DATA IN ASIA**

Project Lead and Editor
Dr Clarisse Girod



ASIAN BUSINESS LAW INSTITUTE

2018

About the Asian Business Law Institute

The Asian Business Law Institute (“ABLI”) is an Institute based in Singapore that initiates, conducts and facilitates research and produces authoritative texts with a view to providing practical guidance in the field of Asian legal development and promoting the convergence of Asian business laws.

DISCLAIMER

Views expressed by the reporters are not necessarily those of the Editor, the Asian Business Law Institute (“ABLI”), Academy Publishing nor the Singapore Academy of Law (“SAL”). Whilst every effort has been made to ensure that the information contained in this work is correct, the reporters, Editor, ABLI, Academy Publishing and SAL disclaim all liability and responsibility for any error or omission in this publication, and in respect of anything, or the consequences of anything, done or omitted to be done by any person in reliance, whether wholly or partially, upon the whole or any part of the contents of this publication.

COPYRIGHT

© 2018 Reporters.

Published by the Asian Business Law Institute under exclusive licence.

All rights reserved. No part of this publication may be reproduced, stored in any retrieval system, or transmitted, in any form or by any means, whether electronic or mechanical, including photocopying and recording, without the permission of the copyright holder.

All enquiries seeking such permission should be addressed to:

The Secretariat
Asian Business Law Institute
1 Supreme Court Lane
Level 6
Singapore 178879
Tel No: (+65) 6332 4388
E-mail: info@abli.asia

ISBN 978-981-11-7311-0



FOREWORD

When I spoke at the launch of the Asian Business Law Institute some two years ago, I said that differences in the legal regimes of the countries in the region posed an impediment to the growth of business. This can clearly be seen in the area of data protection and privacy. Even a cursory glance at the reports in this compendium will reveal that the legal landscape is a patchwork of variegated – and at times conflicting – regulations and stipulations. The challenges that this poses have proven to be a significant hindrance to the development of digital trade and cross-border business operations in Asia.

It is for this reason that the subject of data privacy has been on the agenda of the Institute since its inception. When the Board of Governors of the Institute discussed the project in July 2017, it was decided that the Institute would focus on the regulation of international data transfers, as this has a direct and immediate impact on cross-border business in all of the Asian jurisdictions represented on the Board of the Institute, and in Asia more generally.

Over the past years, the Organisation for Economic Co-operation and Development, the Asia-Pacific Economic Cooperation nations, and the Association of Southeast Asian Nations, among others, have all adopted statements of principle, frameworks or systems recalling the importance of cross-border flows, data protection and privacy. While such supra-national initiatives are useful for the purpose of convergence, they need to be complemented by the hard and prosaic work of sifting through the thicket of national laws and regulations to identify points of commonality and areas where reform is required. From the outset, therefore, the Institute conceived of its Data Privacy Project as proceeding in two stages: first, it would research and study the state of the existing law; second, it would set out to make recommendations to promote greater convergence of national laws and regulations, with the twin goals of upholding privacy and data protection rights and facilitating cross-border trade in the region.

The publication of this compendium of jurisdictional reports – the second in the ABLI Legal Convergence Series – marks the conclusion of the first, descriptive, phase of the project. The reports in this volume have been written by some of the foremost experts on the subject of data privacy in their respective jurisdictions, and they are a truly impressive and unique piece of legal scholarship. Taken together, they offer a comprehensive survey of the regulatory landscape as it relates to cross-border data flows and data localisation obligations in 14 Asian jurisdictions and I have no doubt that they will prove to be valuable resource, not only to practitioners but also to regulators and policymakers both in Asia and beyond, many of whom, I am given to understand, have already expressed an intention to make use of the compendium. I commend this work to anyone with an interest in legal convergence in this area of the law, including governments which are working on drafting or reviewing their own data privacy legislations.

This publication of this compendium also raises the curtain on the second, prescriptive, phase of the project where the Institute will work towards the development of concrete proposals for the introduction of common rules and standards on cross-border data transfers. In this context, it is interesting to note that the reports reveal not only gaps, but also considerable similarities in the legal systems. This is encouraging, for it suggests that there is scope for greater convergence in this complex and fast-evolving area of the law.

The wider objective of the Data Privacy Project is to promote a shared legal ecosystem for international data transfers in Asia that would also be interoperable with those already extant in other regions, such as Europe. There is no question that this is an ambitious goal, but I draw confidence from the fact that it is a shared enterprise. In this context, I would make special mention of the Data Privacy Forum which was organised by the Institute in Singapore on 7 February 2018 and was attended by 90 high-level representatives from governments, data protection agencies, supranational organisations, industry, academia, and the legal community from 19 different jurisdictions. During the Forum, the participants engaged in a fruitful and productive discussion on how a framework for the sharing and transfer information across international borders might be developed in Asia. The breadth and depth of the support which the Institute has enjoyed thus far, together with the quality of this

publication, gives me every confidence that its ambition is backed by the necessary wherewithal to make it a reality.

This project is the work of many hands. Gratitude is due, first and foremost, to the jurisdictional reporters who have so generously agreed to give up their time to lend their considerable expertise to this project. Thanks must go also to the data protection and privacy commissioners and governments who have provided invaluable support and whose participation has greatly increased the stature of the project. Finally, special thanks are due to Dr Clarisse Girot, the project leader, and her team at the Institute and the Singapore Academy of Law for so skilfully co-ordinating the efforts of the jurisdictional reporters and for editing the various chapters. This compendium would not have been possible without the tremendous effort they have put in.

I congratulate the Institute on what has been achieved thus far and I look forward with eager expectation at what is to come.

Sundaresh Menon

Chief Justice

Supreme Court of Singapore

24 April 2018

CONTENTS

	Page
<i>Foreword</i>	iii
Introduction	1
<i>Project Lead and Editor: Clarisse Giro</i>	
Jurisdictional Reports	
Australia	17
<i>Reporter: Peter G Leonard</i>	
China	62
<i>Reporter: Kemeng Cai</i>	
Hong Kong SAR (China)	95
<i>Reporter: Mark Parsons</i>	
India	117
<i>Reporters: Amber Sinha and Elonnai Hickok</i>	
Indonesia	142
<i>Reporters: Justisiari P Kusumah and Danny Kobrata</i>	
Japan	165
<i>Reporter: Kaori Ishii</i>	
Macau SAR (China)	188
<i>Reporter: Graça Saraiva</i>	
Malaysia	215
<i>Reporter: Abu Bakar Bin Munir</i>	
New Zealand	247
<i>Reporter: Katrine Evans</i>	
Philippines	278
<i>Reporter: J J Disini</i>	
Singapore	315
<i>Reporter: Ken Chia</i>	
South Korea	343
<i>Reporter: Kwang Bae Park</i>	

Contents

	Page
Thailand	383
<i>Reporter:</i> David Duncan	
Vietnam	394
<i>Reporter:</i> Waewpen Piemwichai	

INTRODUCTION

Project Lead and Editor: **Dr Clarisse Girod**

Research fellow, Asian Business Law Institute (ABLI)

1 This volume, the second in ABLI's Legal Convergence Series, is a unique compendium of reports on the regulation of cross-border data flows in Australia, the People's Republic of China, Hong Kong SAR, India, Indonesia, Japan, South Korea, Macau SAR, Malaysia, New Zealand, the Philippines, Singapore, Thailand, and Vietnam.¹ Its publication concludes the first phase of ABLI's Data Privacy Project, whose ambition is to contribute to laying the fundamentals for a shared legal ecosystem for cross-border data transfers in the wider Asian region.

2 This publication is significant for at least three reasons. Firstly, this is the first in-depth, bottom-up study that has been undertaken on the regulation of cross-border data flows in Asia. Secondly, the reports have been written by renowned experts in each of the 14 jurisdictions covered in the project, and the majority include the input of the domestic Data Protection Commission or competent Ministry on specific issues that fall within their remit. Thirdly, this publication will be released just as the need for tighter regulation on data sharing and international data transfers has been making the headlines² and as the European General Data Protection Regulation ("GDPR") comes into force, and a few months before the data localisation provisions in the Chinese Cybersecurity Law become applicable – two texts with a major impact on many Asian companies operating internationally. This context enhances the timeliness and relevance of the project and it is hoped, therefore, that this publication can effectively contribute to achieving convergence in this area of law in the region.

1 All reports are current as of 1 April 2018.

2 IAPP Asia Dashboard Digest, "Fallout from Facebook/Cambridge Analytica Could Impact Regulations in Asia" (5 April 2018); "Facebook Scandal Could Push Other Tech Companies to Tighten Data Sharing" *The Straits Times* (22 March 2018).

3 Understanding the direction of ABLI's Data Privacy Project and the purpose of this compendium requires having a full overview of the backdrop against which the project was conceived.

4 As the reports mention on multiple occasions, sharing data across borders has become the lifeblood of all segments of developed and developing economies, particularly in Asia where markets have embraced years of hyper-growth. In fact, a vast number of traditional industries, big or small, now make routine decisions by relying on data from various locations around the world. Small and medium-sized enterprises have become exporters by joining e-commerce marketplaces, whilst crowdfunding, "digital money", mobile payments, wireless transfers, and payment gateways revolutionise the way they start up, accept payments, and go global. Large companies manage their international operations in leaner, more efficient ways.³ Data on customers, suppliers, and employees is increasingly outsourced to overseas third-party providers, especially in cloud computing – be it to gain a competitive advantage or as part of normal business operations, as production is fragmented into global value chains and goods and services are digitised. A variety of business models around the Internet of Things and big data has emerged, which present as many opportunities as challenges.⁴ Building on these trends, Asian jurisdictions compete in their ambitions to become regional or global hubs in business-processing outsourcing, data centres, cloud computing, artificial intelligence, or big data analytics.

5 In a context where data has never been so useful, however, companies operating across Asian borders face a contrasted and constantly shifting legal landscape in data protection and privacy ("data privacy" for short), with a significant impact on cross-border data flows. This compendium thus finds its first utility in its contribution to mapping this diversity and to identifying its causes, albeit impending developments were expected in several jurisdictions even at the date it went to press. In fact, Asia holds some of the most mature, as well as

3 McKinsey Global Institute, "Digital Globalization: The New Era of Global Flows" (March 2016).

4 Big Data Business Models: Challenges and opportunities, Ralph Schroeder, Oxford Internet Institute, Cogent Social Sciences (2016), 2: 1166924.

some of the most recent data protection regimes globally.⁵ Sophisticated data protection legislations including data transfer provisions have been in place since the 1990s in Australia, Hong Kong SAR, Japan, New Zealand, Taiwan, and South Korea, the last of which is considered to have one of the strictest data protection laws in the world. Macau SAR and Association of Southeast Asian Nations (“ASEAN”) countries, namely Indonesia, Malaysia, the Philippines and Singapore have caught up only more recently “to boost the [countries’] competitiveness in the international information economy by providing a legal framework by which personal information shall be handled and transferred”.⁶ Data protection bills are pending in India, Indonesia and Thailand, reportedly also in Vietnam. Law reform has been achieved or is underway in Australia, Singapore, Japan, Korea and New Zealand, whilst the entry into force of data transfer restrictions is under debate in Hong Kong SAR. China has introduced personal information protection requirements in its Cybersecurity Law and implementing regulations, so as to codify and complement similar requirements embodied in existing laws and regulations,⁷ and final guidelines on international transfers are awaited. Specific regulatory controls with a possible impact on data flows are also under review in several countries.

6 As the reports indicate, rule-making on data transfers, whether in data privacy or sectoral laws, will continue to intensify in the region. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (“CPTPP”) signed on 8 March 2018 puts heavy emphasis on the need for data to flow alongside goods and services whose trade has been liberalised, and similar provisions would be included in the Regional Comprehensive Economic Partnership (“RCEP”). The digital economy and trade facilitation are two key economic priorities of the new Singaporean chairmanship of ASEAN, which will translate into initiatives to build up digital connectivity, and facilitate e-commerce

5 See also the book of reference by Graham Greenleaf, “Data Privacy Laws in Asia – Trade and Human Rights Perspectives” (Oxford University Press, 2014).

6 J J Disini, Jurisdictional Report – Philippines, at paragraph 2, quoting Explanatory Note to House of Representatives House Bills.

7 Graham Greenleaf & Scott Livingston, “China’s Personal Information Standard: The Long March to a Privacy Law” (2017) 150 *Privacy Laws & Business International Report* 25.

flows.⁸ Meanwhile, the APEC Cross-Border Privacy Rules (“CBPRs”) and Privacy Recognition for Processors systems are expanding, as additional economies have announced that they would join the system. Following Japan and South Korea, Singapore is currently working on the articulation of an ambitious Data Protection Trustmark certification scheme with the CBPRs.⁹ The reports also demonstrate how, pushed by the extraterritorial effects of the GDPR, European influence is growing.¹⁰ European Union (“EU”) standards guide or inspire reflections on national reforms, for example, in Thailand, India, Indonesia, and Hong Kong SAR,¹¹ and several laws have imported European concepts, for example, “data portability” in the Philippines, or the “right to be forgotten” in Indonesia and South Korea. GDPR guidance has been adopted in nearly all Asian countries.¹² Japan and Korea have amended their laws with the objective of obtaining the recognition of their laws on personal data protection as “adequate” by European standards, with Japan negotiating on the basis of mutual adequacy findings. New Zealand – to date, the only country in this part of the world to have obtained such a decision – is currently updating its Privacy Act in order to ensure that it continues to meet that adequacy standard.¹³ There

8 Lim Hng Kiang, Minister for Trade and Industry of Singapore, opening remarks at the 24th ASEAN Economic Minister’ retreat (1 March 2018).

9 Ken Chia, Jurisdictional Report – Singapore, at paragraphs 89–93.

10 On this regional evolution, see Hogan Lovells’ Asia Pacific Data Protection and Cyber Security Guide 2018 – “Shifting Landscapes across the Asia-Pacific Region” at p 4.

11 “Hong Kong’s Privacy Commissioner to Review Ageing Data Protection Law after ‘Major Data Leaks’” *South China Morning Post* (25 April 2018).

12 See, eg, the European General Data Protection Regulation (“GDPR”) guidance published by the Hong Kong Office of the Privacy Commissioner for Personal Data including a comparison table highlighting the major differences between the GDPR and the Hong Kong Personal Data (Privacy) Ordinance (Cap 486) (2016), the guidance released by New Zealand Trade and Enterprise (September 2017), the factsheet released by the Personal Data Protection Commission of Singapore (2017), etc. Specific guidance has been provided by the European Union’s Article 29 Data Protection Working Party to Asia Pacific Privacy Authorities to assist them in developing their own GDPR guidance to businesses and organisations processing the data of individuals enjoying protection under the GDPR. See <<http://www.appaforum.org/resources/guidance/appa-gdpr-general-information-document.pdf>> (accessed 30 April 2018).

13 Katrine Evans, Jurisdictional Report – New Zealand, at paragraphs 29–31.

would be a great degree of geopolitical and economic interest from both EU and India in granting the latter an adequacy status.¹⁴

7 The reports also reveal the complexity of the task to monitor legal developments in jurisdictions which have made plans to “catch up” on the global privacy debate over the years. In India, Thailand, and Indonesia, plans to adopt data protection laws lay dormant for years before suddenly going through a revival in 2018. A draft Chinese data protection bill initiated in 2003 is regularly mentioned, but it might take another “three to five years” (probably more) to pass into law.¹⁵ Even when legislative plans appear to be firmly on track, in practice, any hopes to expedite legislative processes are quickly dashed. Governments and lawmakers must absorb the complexity of global developments, often under high international and industry pressure but with limited resources, while simultaneously addressing pressing local concerns. For instance, in India, one of the objectives of the data protection bill under discussion is to position India as an international data hub, and another, just as daunting, is to tackle the highly sensitive privacy issues surrounding Aadhaar, the biometrics-based unique identity scheme in which more than a billion Indians have already been enrolled. Moreover, as the reports again show, data privacy laws intersect with specific rules in virtually all sectors – primarily in healthcare, finance, credit reporting, e-commerce and consumer protection, as well as in labour relations. The necessary co-ordination at law and regulatory level is cumbersome, time-consuming, and often an obstacle to regional convergence. Delays are all the more likely when the future Data Protection Act is designed as “comprehensive”, that is, to cover the public sector, like in Indonesia. While countries and regions duplicate the standards of legislation elaborated elsewhere, simply transplanting the law from another jurisdiction (in theory, an effective way of ensuring legal convergence) does not work.¹⁶ No overarching structure of co-operation exists to assist with these matters in the region, and few comparative studies are

14 Amber Sinha & Elonnai Hickok, Jurisdictional Report – India, at paragraph 26.

15 George G Chen & Tiffany G Wong, “Waiting for China’s Data Protection Law” *The Diplomat* (12 August 2017).

16 As an example, see Graça Saraiva, Jurisdictional Report – Macau SAR (China), on the specific challenges raised by the replication of the Portuguese Data Protection Act in local law, at paragraph 3.

available. In reality, regional convergence of data privacy laws is constantly at risk of being pushed down the ladder of government and parliamentary priorities.

8 In several chapters, the compendium describes data localisation policies as another great challenge for companies operating cross-border in the region. With data viewed as a “national basic strategic resource”,¹⁷ an increasing number of Asian countries – mainly, but not exclusively, China, Indonesia and Vietnam – have adopted, or are considering laws requiring that data generated locally on their citizens and residents be kept within their geographic boundaries and remain subject to local laws. The protection of privacy and national security interests, aid to law enforcement, and preventing foreign surveillance, in addition to appeals to the principle of sovereignty, are the classic motives supporting such measures. In contrast, global industry players and foreign governments claim that some of these laws in fact aim at protecting local markets and tech champions, possibly in violation of commitments in agreements such as the General Agreement on Tariffs and Trade, which covers some affected services.¹⁸ The CPTPP includes onerous requirements on any parties which have (or are considering) data localisation laws, but the same issues are reported as creating tensions in negotiations on the e-commerce chapter of the RCEP – with disputes around the evidence of the negative impacts of data localisation on gross domestic product, and the argument that free data flows discourse would enable the perpetuation of an existing unequal global economic order. Whatever the rationales behind these policies and trade disputes, in the meantime, local businesses are restricted in their ability to take advantage of technologies such as cloud computing, and companies face inflated costs of using or building data centres in-country, which may raise challenges due to lack of adequate infrastructure. These requirements may thus impede the

17 Yanqing Hong, *The Cross-Border Data Flows Security Assessment: An Important Part of Protecting China's Basic Strategic Resources*, Working Paper, 20 June 2017 <<http://apide.org/apru-asia-eu-dialogue/readings/CrossBorderDataFlows.pdf>> (accessed 30 April 2018).

18 Communication (S/C/W/374) circulated to the members of the Council for Trade in Services of the World Trade Organisation (23 February 2018).

digital economy and the growth of telecom and Internet services.¹⁹ Moreover, the scope of the laws is often uncertain as the definitions of key legal notions can be in flux.²⁰

9 Most of the reporters of these reports express the view that this combination of patchy laws and of a shifting regulatory environment is a source of business concern, “without it necessarily being the case that data subjects’ interests are demonstrably advanced through, for example, improved data security or regulatory oversight”.²¹ In fact, full compliance can never be guaranteed, even as enforcement is taking off, penalties are increasing, and data protection regulators are setting up regional and international networks to support joint enforcement initiatives. Key decision-makers across corporate Asia have mentioned compliance and adapting to new regulations as the biggest challenge facing Asian businesses in 2018,²² with the emergence of new laws created to regulate a growing digital economy in Asia, including data privacy, as a key driver behind this concern.²³

10 Supra-national organisations have weighed in for a better alignment of national rules with an impact on cross-border data transfers. In the year 2016 alone, among others, the United Nations Conference on Trade and Development (“UNCTAD”) released a substantive report to that effect,²⁴ and the World Bank Group called for countries to enact data

19 Waewpen Piemwichai, Jurisdictional Report – Vietnam, on the draft Cybersecurity Law, at paragraph 4.

20 Kemeng Cai, Jurisdictional Report – China, *eg*, on the notions of “network operators” and “important data”, and the scope of “security assessments processes” in the Chinese cybersecurity Law; Justisiari P Kusumah & Danny Kobrata, Jurisdictional Report – Indonesia, on the notion of “public service” in GR 96/2012, at paragraph 44.

21 Mark Parsons, Jurisdictional Report – Hong Kong, at paragraph 9.

22 Baker McKenzie’s Asia Pacific Business Complexities Survey 2017, “Simplifying Business in a Complex World: Business Challenges and Legal Solutions in Asia Pacific”.

23 LegalTech News, “Digital Growth Set to Squeeze Region’s Corporate Counsel”, <<https://www.law.com/legaltechnews/almID/1202782931118/>> (accessed 20 April 2018).

24 United Nations Conference on Trade and Development, “Data Protection Regulations and International Data Flows: Implications for Trade and Development” (2016).

protection regulations following internationally recognised principles, “so that multinational companies do not avoid the country because of uncertainty about compliance and trust in the handling of data”.²⁵ A few months later, building on the APEC Privacy Framework of 2005, revised in 2015, the ASEAN Economic Community (“AEC”) adopted its Framework for Data Protection to promote co-operation between AEC members in the implementation of the same Principles of Personal Data Protection in their domestic laws and regulations.

11 In fact, the reports show how a majority of Asian governments, lawmakers and regulators have effectively worked to implement these high-level principles into their national legal systems over the past years. Yet, this transposition has not achieved the desired objective of regional consistency. In reality, while frameworks such as the APEC and ASEAN data privacy frameworks have provided “rough signposts for a common approach to principles-based regulation”, “moving from a plain reading of the text of the newly enacted data protection laws (which in many respects appear similar across the region) to the practicalities of enforcement and compliance, we actually see increasing divergence as jurisdictions prescribe more and more detailed requirements, often with local nuance”.²⁶

12 Provisions on international data transfers in data privacy laws offer a typical example of variations in local requirements adopted to implement common principles. Since their early adoption in 1980, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data have articulated this balancing act around a principle of free flow of data and the admission that restrictions may be legitimate, where the country of destination “does not yet substantially observe” the Guidelines or “where the re-export of such data would circumvent its domestic privacy legislation”. The Guidelines, revised in 2013, have set common standards for OECD Member Countries to shape their laws and regulations on cross-border data flows, while also insisting on the crucial need to address the global dimension of privacy through improved

25 World Bank World Development Report, Global Cooperation 2016.

26 Patrick Sherrington, “Data Protection and Cyber Security Regulation: Shifting Landscapes Across The Asia-Pacific Region” *Conventus Law* (25 April 2016).

“interoperability” of privacy regulations. As for the Additional Protocol to the Council of Europe Convention 108, the only internationally binding data protection instrument to date, it provides that data may only be transferred to a third party to the Convention “if the recipient State or international organisation is able to afford an adequate level of protection”, or if “adequate safeguards, in particular resulting from contractual clauses, are provided by the data exporter in accordance with domestic law”. Similar provisions are found in the EU Data Protection Directive 95/46/EC, now in the GDPR.

13 As the reports show, the implementation of this balancing test in Asian legal systems has resulted in a patchwork of varying laws and implementing regulations. Data localisation rules aside, all jurisdictions in principle allow cross-border data transfers to take place. However, they do so under conditions that differ between jurisdictions. Default positions may vary, as transfers may be either authorised or prohibited as a rule, with exceptions in either case. The laws provide various instruments to comply with cross-border data transfer requirements in each jurisdiction (namely, contracts, certification and trustmarks, CBPRs, binding corporate rules, countries put on “white lists”, *etc*), but not all of these are replicated, or their implementation might be different or uncertain in the other jurisdictions. For instance, there is no regionally shared criteria for white lists.²⁷ The individual’s consent plays a prominent role in all legal systems, but with varying importance: whilst the user’s consent is one of several bases for transfers in most countries, it is in principle a systematic prerequisite for transfers from Korea. Moreover, the very notion of consent may be construed differently from one jurisdiction to another, running the gamut from express informed consent given in writing to implied consent understood as failing to opt out in certain circumstances. The resulting paradox is that, in Korea, whilst the under-development of the online marketing or big data

27 On this issue, see Abu Bakar Bin Munir, Jurisdictional Report – Malaysia, discussing the criteria mentioned in the draft white list issued for consultation by the Commissioner for Personal Data Protection of Malaysia in April 2017, at paragraphs 65–75 and Kaori Ishii & Fumio Shimpo, Jurisdictional Report – Japan, on the “judgmental standards” set by the Japanese Personal Information Protection Commission to consider whether to put specific countries on a “white list”, at paragraphs 54–58.

industries in comparison with the country's well-established technology infrastructure is, in part, attributed to the demanding opt-in consent requirements,²⁸ on the contrary, there would be little demand at present for alternative mechanisms in Thailand, for instance, because capturing consent is not considered as too burdensome.²⁹ Public authorities are given different enforcement and administrative roles in the implementation of these regulations, and no mechanism of regulatory co-ordination or mutual recognition exists to facilitate multi-jurisdictional compliance. In practice, provisions on data transfers are hardly ever enforced, if at all – which can, in part, be attributed to the fact that “invasions of data privacy are difficult to detect because they can be invisible”,³⁰ specifically when they occur in a transborder context.

14 ABLI's stance is that this apparent paradox – the adoption of overarching common principles leading to contradictions in national laws, to the point of negating the benefits of convergence efforts – is, to a large extent, owed to the lack of an *ad hoc*, comprehensive structure of regional co-operation in data privacy that can assist to ensure the consistent implementation of regional standards on data privacy at the national level.

15 In this context, how can ABLI contribute? As a neutral, multi-stakeholder research institute with a pan-Asian focus, at the launch of the project in July 2017, ABLI considered itself in an ideal position to help fill the gap between national developments and regional initiatives to build a trusted digital ecosystem in Asia. It thus set its aim on the development of recommendations on the convergence of rules on cross-border data transfers and their implementation in Asia to assist companies in their compliance efforts, governments and regulators in the development of consistent policies in cross-border data flows and to offer a referential for Asian jurisdictions that are considering putting or reviewing cross-border controls in place. These recommendations would thus be a first step to support legal convergence in the field of data

28 Kwang Bae Park, Jurisdictional Report – South Korea, at paragraph 4.

29 David Duncan, Jurisdictional Report – Thailand, at paragraph 29.

30 *Puttaswamy v Union of India*, available at <<https://indiankanoon.org/doc/91938676/>> (accessed 30 April 2018).

privacy in the region, which could be taken over for practical implementation in other fora.

16 It is from this perspective that this compendium was conceived. As set out above, its first objective is to provide detailed information on the state of the law in all the jurisdictions covered in this study. Beyond this first objective, however, the compendium offers prime material to identify the key issues on which the laws do or do not differ and highlight the common relevance of specific regional or global developments for all legal systems.

17 The in-depth study of these differences and commonalities, and – where feasible – the drafting of recommendations and/or policy options to achieve convergence, will form the second part of the project. However, several preliminary observations can be made from a first-level analysis of the reports, which will be helpful to guide this future work.

18 A first observation issued from the reports is in respect of the profound importance awarded to data privacy throughout the region, in domestic as well as in cross-border dealings. This significance becomes increasingly visible in all legal systems surveyed. A framework for privacy is in place - with variations – in the Constitutions or Basic Laws of Hong Kong SAR, Indonesia, Japan, Korea, Macau SAR, the Philippines, Thailand, and Vietnam, as well as in other countries not covered in this study such as Cambodia and Myanmar.³¹ Important cases have also been handed down on the basis of constitutional privacy provisions in Indonesia, Japan and Korea, and more recently in India, where the Supreme Court has read the right to privacy of 1.35 billion individuals into the right to life and liberty and Part III (Chapter on Fundamental Rights) in the Constitution, which has re-ignited the process towards the adoption of a Data Protection Act. Australia, Malaysia, New Zealand and Singapore do not recognise privacy as a fundamental right but protect data privacy through strong statutory enactments, enforced by the data protection authorities and the courts. Furthermore, even in jurisdictions where data privacy is not recognised as a constitutional

31 Myanmar Centre for Responsible Business, *Sector-Wide Impact Assessment of Myanmar's ICT Sector* (24 September 2015) ch 4:3.

right, it is considered a key value to develop trust, a *sine qua non* condition which would explain why the digital economy is currently kept from growing in several parts of the world.³² A recent CCTV-Tencent survey has reinforced the view that Chinese consumers are becoming more aware and vocal about their privacy and how their personal data is used.³³ Korea, Japan, as well as China and Singapore are counted among the countries that have increased their participation in the debate on ethics and the development of artificial intelligence, originally largely a “Western” discussion.³⁴ In fact, the reports provide countless examples which concur with studies rebutting the argument that Asian data privacy laws, despite different justifications, would deviate from supranational instruments by virtue of the fact that these have mostly been drafted in “the West”.³⁵ If this argument was ever valid, then the causes for legal divergence in this area of law would certainly be found elsewhere today.

19 The second observation is that, read together, the reports clearly show how three different regulatory models are shaping national data protection frameworks in Asia – at the risk of oversimplification, one is mainly driven by concerns of data sovereignty, national security, and the big data-driven economy (“Chinese model”), another is articulated around the recognition of privacy as a fundamental human right (“European model”), and another implements a more liberal, market-driven approach to regulation (“American model”). In contrast to other parts of the world, these three models find themselves operating concurrently in Asia as countries expand their range of trading partners in the region. A view shared by most reports is that sustainable

32 Findings of the 2017 CIGI-Ipsos Global Survey on Internet Security and Trust, undertaken by the Centre for International Governance Innovation and conducted by Ipsos in collaboration with the United Nations Conference on Trade and Development and the Internet Society.

33 “The Increasing Use of Artificial Intelligence Is Stoking Privacy Concerns in China” *South China Morning Post* (5 March 2018).

34 “Robots Bring Asia into the AI Research Ethics Debate” *University World News* (24 November 2017).

35 Privacy International, “A New Dawn: Privacy in Asia” (December 2012) at p 2; see also Graham Greenleaf, “Values and Interests in Asian Data Privacy Protection” in *Data Privacy Laws in Asia – Trade and Human Rights Perspectives* (Oxford University Press 2015) and at pp 17–22.

convergence in this area of law will only be achieved if a high level of data privacy protection is implemented in the legal systems of the region, and that, for various reasons, it appears likely that the requirements of the EU's GDPR will become the default standard emerging from this "race to the top". However, some reporters question whether the GDPR approach to cross-border data transfers is the optimal policy approach,³⁶ and some jurisdictions will certainly remain intent on implementing different standards. How these different models interact, and whether and how national laws can effectively enable them to be "interoperable" will be a common thread for the second part of the project.

20 The third observation relates to the direction which ABLI has set for the Data Privacy Project, and to the scale of issues which it has consequently chosen to address. From the outset, the project has been designed to go beyond a mere study of data transfer provisions in Asian data privacy laws, and to address the wider spectrum of issues that have an impact on the legal framework of cross-border data flows. They have been organised around five key themes:

- (a) the legal and business risks of inconsistencies and gaps in coverage in Asian data protection laws;³⁷
- (b) the legal challenges attached to data localisation requirements in Asia;
- (c) the practical implications of data-related clauses in international trade agreements and treaties for Asian legal systems;
- (d) the implementation of data transfer mechanisms and consent requirements in Asian data privacy laws; and
- (e) the role and powers of the privacy enforcement authorities in the regulation of international transfers and international co-operation.

36 See, eg, Peter G Leonard, Jurisdictional Report – Australia, at paragraphs 11–12.

37 On this point, see the synthetic recension of these gaps done by Prof Graham Greenleaf for ABLI's Data Privacy Forum – *The Legal and Business Risks of Inconsistencies and Gaps in Coverage in Asian Data Protection Laws*, Research Paper No 21, 7 February 2018 <<https://ssrn.com/abstract=3119441>> (accessed 30 April 2018).

21 These issues were selected with input from the jurisdictional reporters, public and private stakeholders across the region, and based on recommendations of organisations such as UNCTAD and the International Conference of Data Protection and Privacy Commissioners. They are consistently addressed in the reports so as to enable comparisons and also formed the basis of discussions at the Data Privacy Forum hosted by ABLI in Singapore on 7 February 2018.³⁸ Their relevance for all Asian legal systems has been confirmed on multiple occasions. For all these reasons, it is envisaged that they will form the core of the second phase of the project.

22 There is no doubt that the project is ambitious and that many challenges lie ahead. But the genuine desire for convergence and the interest in the Data Privacy Project which ABLI has witnessed over the past months certainly create the right conditions for the project to bear fruit. The publication of this compendium is in effect a sign that legal convergence in this area of law is a shared objective.

23 This publication is, thus, a pivotal step in ABLI's Data Privacy Project. It is also a gratifying achievement that materialises the work and effort put into ABLI's Data Privacy Project by its many contributors over the past months.

24 I wish to express my special gratitude to the 17 reporters of these reports, who have accepted to embark on this unprecedented initiative when it was in its embryonic stage. Their willingness to freely lend their time and expertise is a token of the relevance of the project for the region, and I hope to carry our collaboration further as the project reaches a more challenging phase.

25 The contributions of the Data Protection and Privacy Commissions of the region to the project must also be acknowledged. Their support of ABLI's initiative has been a key incentive for setting ambitious goals to the project. I wish to address special thanks to Commissioner Tan Kiat How, Chairman Leong Keng Thai, and Deputy Commissioner Yeong

38 See <<http://abli.asia/NEWS-EVENTS/Whats-New/ID/52>> (accessed 30 April 2018).

Zee Kin of the Personal Data Protection Commission of Singapore, to Stephen Kay-yi Wong, Privacy Commissioner for Personal Data of Hong Kong SAR, to John Edwards, Privacy Commissioner of New Zealand, and to Ivy Patdu, Deputy Privacy Commissioner of the Philippines, for personally attending ABLI's Data Privacy Forum in Singapore on 7 February 2018. The representation of the Personal Information Protection Commission of Japan, Korean Communications Commission, Korea Internet & Security Agency, Office of the Commissioner for Personal Data Protection Commission of Malaysia, and of the governments of Vietnam, Indonesia, Cambodia, Singapore, Thailand, and of several supra-national organisations was also highly appreciated. I also thank the Secretariat of the International Conference of Data Protection and Privacy Commissioners for granting ABLI discretionary access to the results of the first census undertaken among the conference members in 2017. These results have been used to draft the questionnaire on the basis of which the jurisdictional reporters have written their reports.

26 The Institute is also indebted to the many representatives of industry, trade associations, law professions, and academia, who provided invaluable input, especially to Prof Graham Greenleaf of the University of New South Wales and Prof Sinta Dewi of Universitas Padjadjaran, the management committee and members of AsiaDPO, Rahul Sharma of the Perspective, and Dr Yanqing Hong of Peking University.

27 The team of Academy Publishing deserves much praise for its kind patience and professionalism, as does Sung Yu Xin, who has put her many skills to the service of ABLI in reviewing these reports and lending a helpful hand in the organisation of ABLI's Data Privacy Forum. I wish her well on her project of a future career in the fascinating field of data protection and privacy.

28 Prof Yeo Tiong Min, Academic Director, Sarah Archer, Mark Fisher and Kwok Wai Meng, the team of ABLI's Secretariat, will only be mentioned briefly, as their support deserves more thanks than can be expressed on this page.

29 Finally, I wish to express my gratitude to the Board of Governors of ABLI for placing their confidence in me, a relative newcomer to Asian shores, to lead this project.

Jurisdictional Report

AUSTRALIA

Reporter: **Peter G Leonard**
Principal, Data Synergies

A INTRODUCTION

1 Australian data privacy statutes do not preclude or significantly restrict international data flows. Instead, Australian data privacy regulation imposes a requirement of “accountability” of entities that are regulated by Australian data privacy laws and “disclose” personal information to recipients outside Australia to ensure that recipients of that personal information which are not regulated by Australian data privacy laws handle that personal information consistently with the requirements of Australian data privacy laws.

2 Australia is a federation with relevant data protection statutes in operation at both the federal (sometimes referred to as “Commonwealth of Australia” or simply “Commonwealth” or “Australian”) and state and territory levels of government. Each of these statutes is derived directly or indirectly from the Organisation for Economic Co-operation and Development (“OECD”) “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, as first published in 1980 and reviewed and updated in 2013¹ (“OECD Privacy Guidelines”). The 2013 version of the OECD Privacy Guidelines is substantially similar to the 1980 version, but with added detail around transborder controls and international co-operation. The 1980 version of the OECD Privacy Guidelines was developed in a pre-Internet computing era, in response to business concerns that cross-border information flows, particularly in the

1 Revised Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD Privacy Guidelines) as adopted on 11 July 2013 by the Organisation for Economic Co-operation and Development Council, available at <www.oecd.org/sti/ieconomy/privacy-guidelines.htm> (accessed 6 April 2018).

banking, finance and insurance sectors, were being impeded because states were reluctant to permit their citizens' personal information to be sent across territorial borders unless the receiving state protected the information in the same manner as the sending state. To address this problem, the OECD Privacy Guidelines proposed an information privacy framework that protected information privacy whilst also promoting the free flow of information. The OECD Privacy Guidelines sets out a set of principles for the fair handling of personal information, including a so-called "accountability principle" (Principle 16). This principle requires organisations that collect personal information and transfer that personal information to a recipient outside the jurisdiction to be accountable for the recipient meeting the principles for the fair handling of personal information, in addition to (and regardless of) the requirements of data protection laws of the recipient's jurisdiction. The "accountability principle" as enacted in the Privacy Act is directly derived from the OECD's stated "accountability principle".

3 The federal Privacy Act 1988 ("Privacy Act") is the principal privacy statute in Australia. This Privacy Act includes the Australian Privacy Principles² ("APPs") and which have mandatory operation. The federal Privacy Act operates across all sectors of the Australian economy except activities of state and territory government agencies. The Privacy Act regulates collection, use, disclosure and retention by "APP entities" of "personal information" that is collected for inclusion in any form of print or electronic "record" or in a "generally available publication". Generally, the federal statute applies to all businesses (except small business enterprises) operating in Australia, and also to Australian established in Australia in relation to their operations outside Australia. We address later in this report how to determine whether an organisation is an APP entity and when the Privacy Act operates extraterritorially.

2 See Sch 1 of the Privacy Act 1988. Information on the Australian privacy principles may also be obtained from the Office of the Australian Information Commissioner's website <<https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles>> (accessed 6 April 2018).

4 The stated objects of the Privacy Act include facilitating the free flow of information across national borders while ensuring that the privacy of individuals is respected (section 2A(f)). As to cross-border transfer of personal information, the key relevant provision is Australian Privacy Principle 8 (“APP 8”) – “Cross-border disclosure of personal information”.

5 The Privacy Act is administered by the Australian Privacy Commissioner within the Office of the Australian Information Commissioner (“OAIC”). Although the APPs are stated at a relatively high level of generality, other parts of the Privacy Act follow the relatively detailed, prescriptive and mandatory form that is the customary drafting style of Australian statutes. The Australian Privacy Commissioner may make public interest determinations relaxing the operation of provisions of the Act in particular circumstances and for specified persons or classes of persons and then only after following public consultation procedures. Otherwise the Australian Privacy Commissioner has limited powers to determine or prescribe the future development of privacy regulation. In particular, regulation of cross-border data flows is largely dictated by operation of provisions of the Privacy Act, rather than through exercise of regulatory discretion by the Australian Privacy Commissioner.

6 However, the Australian Privacy Commissioner is empowered to issue guidelines as to the operation of the Privacy Act. In February 2014, the Privacy Commissioner first released the “Australian Privacy Principles Guidelines” (“APP Guidelines”), as subsequently amended and updated.³ Chapter 8 of the APP Guidelines addresses the requirements of APP 8. This is the most comprehensive statement of the Privacy Commissioner’s interpretation of APP 8, which is the key provision addressing cross-border data flows. As stated by the Privacy Commissioner: “The APP guidelines outline the mandatory requirements of the APPs, how the Privacy Commissioner will interpret the APPs, and matters we may take into account when exercising functions and powers under the Privacy Act.” The APP Guidelines does

3 See <<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/>> (accessed 6 April 2018).

not have formal legislative status. However, the APP Guidelines is of significant interest as an expression of the Privacy Commissioner's interpretation of key provisions of the Privacy Act. The APP Guidelines can reasonably be expected to be applied by the Commissioner as the enforcement authority for the Act. The APP Guidelines can also be expected to be taken into account by the courts in any review of enforcement action taken by the Privacy Commissioner as an important statement of authority as to interpretation of key provisions of the Privacy Act, while not binding the court.

7 As already noted, the stated objects of the Privacy Act include facilitating the free flow of information across national borders while ensuring that the privacy of individuals is respected (section 2A(f)). For at least 30 years, there has been broad political and business consensus in Australia that promotion of free trade in goods and services across national borders is beneficial both to the international community and to Australia's national interests. Reduction of barriers to flows of information has been seen as an important part of promotion of trade in goods and services across national borders.

8 In general, Australian governments and policymakers apply a presumption in favour of facilitating free trade in goods and services and associated free flow of information unless a public interest demonstrably requires control of that trade or flow of information, and then limit the extent of controls or restrictions to the level necessary to address that public interest. Regulation by Australian governments of information flows is generally regarded as only required in exceptional circumstances, such as:

- (a) to protect rights of Australian citizens, including as to uses and disclosures of personal information about individuals where the interests of those individuals may be adversely affected by personal information about those individuals being transferred to or collected and held within jurisdictions that do not afford protections that are substantially similar to the APPs or which do not provide practical and accessible mechanisms for Australian individuals to obtain the benefit of protections substantially similar to the APPs;
- (b) to detect and control transnational crime, or conduct of criminal activities within Australia, including fraud, money laundering,

- tax evasion, modern slavery and exploitation of children, and planning and funding of terrorist activities;
- (c) to avoid adverse effects upon national security interests, such as avoiding creation of vulnerabilities in critical national infrastructure such as the financial sector (and in particular payments and securities clearing systems) and operation of broadband communications and other telecommunications networks, and limiting use of encrypted communications which cannot be reasonably monitored by Australia laws enforcement agencies.

9 The accountability principle as applied in Australia has the advantage that regulation is neutral as between handling personal information within a country or outside that country's borders, in that the entity electing to implement the cross-border data transfer is responsible for ensuring compliance with that country's (that is, the data exporter's country) data protection requirements regardless of where or by whom that personal information is held or processed outside that country and the data protection requirements of that data importer's country.

10 By contrast, lack of harmony between privacy laws in the region and some data localisation requirements add to compliance costs and occasionally lead to businesses adopting sub-optimal data architectures in order to meet local law requirements. Diversity in local law requirements also inhibits efficient use of cloud platform services to provide application services to consumers and to manage administration of businesses across the region. Compliance with cross-border data controls generally adds additional costs of doing business without significantly increasing protection of affected individuals or otherwise delivering benefits to the local economy.

11 Some cross-border data transfer systems of regulation facilitate data transfers and reduce friction to trade in services. The accountability principle and like systems of regulation impose burdens which can be discharged through downstream steps and controls that are able as a matter of practice to be discharged where the relevant entity is able to make key data architecture decisions reflecting requirements of the country which imposes those burdens: most particularly, where those burdens are imposed in the country where that entity has its central

management and control. The accountability principle as applied in Australia has the advantage that regulation is neutral as between handling personal information within Australia or transferring that information to and handling that information within a recipient (downstream) country.

12 However, where there is a further upstream country that imposes more prescriptive requirements, such as the European Union's ("EU") General Data Protection Regulation ("GDPR"), relevant to transnational operations of a business entity or business group, it is necessary to repeat those more prescriptive requirements in downstream arrangements in order to discharge the upstream requirements. This has the effect that more prescriptive requirements tend to become the norm for organisations seeking to operate across multiple borders, even where those more prescriptive requirements may not better manage and mitigate information privacy risks. In the current global privacy regulatory environment, unless political support grows for international comity through mutual recognition of multiple cross-border data transfer systems, it appears likely that the requirements of the EU's GDPR will become the default international standard, regardless of whether the GDPR approach to cross-border data transfer is the optimal policy approach.

B LEGAL FRAMEWORK OF INTERNATIONAL DATA TRANSFERS IN AUSTRALIAN LAW

i *Statutory protections over constitutional protections of privacy*

13 The Australian Constitution does not include a reference to data protection or privacy. There is judicial authority that there is no general right of privacy of individuals in Australia. In the seminal Australian case regarding common law privacy rights, *Australian Broadcasting Corp v Lenah Game Meats*,⁴ the High Court of Australia refrained from recognising a separate right to privacy, but left open the possibility of development of a new tort of invasion of privacy. Since *Lenah*, only two

4 (2001) 185 ALR 1.

lower courts have recognised a tort of invasion of privacy: *Gross v Purvis*⁵ in the District Court of Queensland and *Doe v Australian Broadcasting Corp*⁶ in the County Court of Victoria. The future direction of development of a new tort of invasion of privacy in Australia remains unclear.

14 Such rights of Australian citizens and residents as exist in relation to information privacy are through *domestic statutory enactments* that create rights of information privacy directly enforceable by Australian consumers. In some cases, these domestic statutory enactments reflect provisions of international treaties and international agreements to which Australia is a party. Australian citizens and residents do not have a direct right of enforcement of international treaties and conventions to which Australia is a party or has acceded and are dependent upon domestic enactment of corresponding protections.

ii Influence of international data protection frameworks

15 The preamble to the federal Privacy Act notes that Australia is a party to the International Covenant on Civil and Political Rights, the English text of which is set out in Schedule 2 to the Australian Human Rights Commission Act 1986. Australia undertook “to adopt such legislative measures as may be necessary to give effect to the right of persons not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence”.

16 The preamble to the federal Privacy Act also notes that Australia is a member of the OECD, that the Council of the OECD recommended that Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in Guidelines annexed to the Council’s recommendation, and that Australia had informed the OECD that it will participate in the recommendation concerning the OECD Privacy Guidelines. As already noted, the “accountability principle” as enacted in the Privacy Act by

5 [2003] QDC 151.

6 [2007] VCC 281.

2014 amendments is directly derived from the 2013 version of the OECD Privacy Guidelines.

17 Australia is a member of the Asia-Pacific Economic Cooperation (“APEC”). The OAIC is a privacy enforcement authority (“PEA”) participating in the APEC Cross-border Privacy Enforcement Arrangement (“CPEA”). Australia has announced its intention to participate in the APEC Cross-Border Privacy Rules (“CBPR”) system but as at 22 January 2018 had not announced formal lodgment of a Notice of Intent. This announcement of intention followed a public consultation as to whether to participate in the APEC CBPR system.⁷

18 Australia is an observer to the relevant Consultative Committee of Council of Europe Convention 108.⁸

19 Australia has neither applied for an adequacy determination, nor announced any intention to apply for an adequacy determination, under European data protection regulation. The matter has been reviewed on a number of occasions, including when a reference was given by the Australian federal government to the Australian Law Reform Commission (“ALRC”) to comprehensively review Australia’s Privacy Act 1988 in 2006.

20 The extraterritorial effects of the European GDPR are likely to have a significant impact on the data processing activities of businesses in Australia. Australian businesses will need to comply with the GDPR if they: have an establishment in the EU (regardless of whether they process personal data in the EU), or do not have an establishment in the EU, but offer goods and services or monitor the behaviour of individuals in the EU. The GDPR and Australian federal Privacy Act have many similar requirements. Both laws foster transparent information handling

7 Consultation paper at <<https://www.ag.gov.au/Consultations/Documents/APEC-Cross-border-privacy-rules/Australia-and-the-APEC-CBPR-system-paper.DOCX>> (accessed 6 April 2018); submissions and announcement at <<https://www.ag.gov.au/Consultations/Pages/APEC-cross-border-privacy-rules-public-consultation.aspx>> (accessed 6 April 2018).

8 <<http://rm.coe.int/list-of-observer-status-t-pd-july-2017/1680734cae>> (accessed 6 April 2018).

practices and business accountability. Both laws require businesses to implement measures that ensure compliance with a set of privacy principles. Both laws take a privacy by design approach to compliance. Data breach notification is required in certain circumstances under the GDPR and under the Privacy Act (from February 2018). Privacy impact assessments, mandated in certain circumstances under the GDPR, are expected in similar circumstances in Australia. Both laws are technology neutral, which will preserve their relevance and applicability in a context of continually changing and emerging technologies. The Australian Privacy Commissioner has outlined relevant similarities and differences in “Privacy business resource 21: Australian businesses and the EU General Data Protection Regulation”.⁹

iii Privacy and data protection in the federal legislation and laws of Australian states and territories

21 Privacy and data protection regulation is shared between federal jurisdiction (“Commonwealth of Australia” or “Australian Parliament”), the six states (New South Wales, Victoria, Queensland, South Australia, Western Australia and Tasmania) and two territories (Australian Capital Territory and Northern Territory). A useful short background paper on Australian privacy laws is available on the website of the Commissioner for Privacy and Data Protection of Victoria.¹⁰

22 The relevant statutes and instruments are as follows:

- (a) At the federal level, as already noted, the principal statute regulating collection, use, storage and disclosure of “personal information” is the federal Privacy Act and in particular the 13 APPs which form part of that Act. The federal Privacy Act applies to the collection and handling (use, storage and disclosure) of personal information by, amongst others,

9 <<https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation>> (accessed 6 April 2018).

10 <https://www.cdpd.vic.gov.au/images/content/pdf/privacy_papers/Privacy_Background_paper.pdf> (accessed 6 April 2018).

Australian federal government agencies and most private sector organisations (collectively called “APP entities”).

- (b) In New South Wales (“NSW”), the Privacy and Personal Information Protection Act 1998 (NSW) and Health Records and Information Privacy Act 2002 (NSW), as administered by the NSW Information and Privacy Commission.¹¹ These statutes regulate the handling of personal information by NSW public sector agencies and providers of health services in NSW and those providers’ subcontractors.
- (c) In Victoria, the Privacy and Data Protection Act 2014 (Vic) as administered by the Office of the Victorian Information Commissioner¹² and the Health Records Act 2001 (Vic) as administered by the Victorian Health Complaints Commissioner.¹³ These statutes regulate the handling of personal information by Victorian public sector agencies and providers of health services in Victoria and those providers’ subcontractors.
- (d) In Queensland, the Information Privacy Act 2009 (Qld) as administered by the Queensland Office of the Information Commissioner.¹⁴ This statute regulates the handling of personal information by Queensland public sector agencies.
- (e) In South Australia, the Department of the Premier and Cabinet Circular, PC012 – Information Privacy Principles Instruction, 16 September 2013. This is an administrative instruction issued by the South Australian government requiring government agencies to generally comply with a set of information privacy principles. The Privacy Committee of South Australia¹⁵ is responsible for overseeing the implementation of the Information Privacy Principles Instruction by South Australian public sector agencies. The Privacy Committee reports to the

11 <<https://www.ipc.nsw.gov.au/>> (accessed 6 April 2018).

12 <<https://www.cdp.vic.gov.au/index.php>> (accessed 6 April 2018).

13 <<https://hcc.vic.gov.au/>> (accessed 6 April 2018).

14 <<https://www.oic.qld.gov.au/>> (accessed 6 April 2018).

15 <<https://www.archives.sa.gov.au/content/privacy-committee-sa>> (accessed 6 April 2018).

- relevant South Australian Minister and provides advice on privacy issues.
- (f) In Tasmania, the Personal Information and Protection Act 2004 (Tas), administered by the Tasmanian Ombudsman.¹⁶ This statute covers the Tasmanian public sector including the University of Tasmania.
 - (g) In Western Australia, the state public sector does not currently have a statutory privacy regime. Various confidentiality provisions cover government agencies and some privacy principles are provided for in the Freedom of Information Act 1992 (WA) overseen by the Office of the Information Commissioner (WA).¹⁷
 - (h) In the Australian Capital Territory (“ACT”), the Information Privacy Act 2014 (ACT) which regulates the handling of personal information by ACT public sector agencies, and the Health Records (Privacy and Access) Act 1997 (ACT) which regulates the handling of health information by providers of health services in the ACT and those providers’ subcontractors. The Office of the Australian Information Commissioner is currently exercising some of the functions of the ACT Information Privacy Commissioner.¹⁸
 - (i) In the Northern Territory, the Information Act 2002 (NT) as administered by the Information Commissioner for the Northern Territory.¹⁹

iv Transborder data flows under federal Privacy Act (APP8) and OECD Guidelines – “Accountability principle” and “accountability liability”

23 APP 8 and section 16C of the Privacy Act regulate the cross-border disclosure of personal information to recipients outside of Australia. Before “disclosing” personal information to an overseas recipient,

16 <<http://www.ombudsman.tas.gov.au/>> (accessed 6 April 2018).

17 <<http://foi.wa.gov.au/>> (accessed 6 April 2018).

18 <<https://www.oaic.gov.au/privacy-law/other-legislation/australian-capital-territory-privacy>> (accessed 6 April 2018).

19 <<https://infocomm.nt.gov.au/>> (accessed 6 April 2018).

APP 8.1 requires an APP entity to take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to that information. This “accountability principle” will apply where APP 8.1 applies to the disclosure, and the overseas recipient is not subject to the APPs, but the act or practice would be a breach of the APPs if the overseas recipient were subject to the APPs.

24 As already noted, the accountability principle as applied in transborder data flows in APP 8 broadly reflects the approach to “accountability” as recommended by the OECD in the revised OECD Privacy Guidelines as adopted on 11 July 2013 by the OECD Council.²⁰ More contentiously, Australia also applies what is referred to in this report as “*accountability liability*”, through the operation of section 16C of the Privacy Act.

25 Relevantly, paragraph 15(a)(i) of the OECD Privacy Guidelines specifies that a data controller’s *privacy management programme* should give effect to the Guidelines “for all personal data under its control”. The term “control” refers back to the definition of a “data controller”, as defined in paragraph 1(a) and has the effect that a privacy management programme should not only address the data controller’s own operations, but all operations for which it may be accountable – regardless of to whom data are transferred. For example, a privacy management programme should include mechanisms to ensure that agents of the data controller maintain appropriate safeguards when processing personal data on its behalf. Safeguards may also be necessary in relationships with other data controllers, particularly where the responsibility for giving effect to the Guidelines is shared.

26 The Supplementary Explanatory Memorandum to the 2013 version of the OECD Privacy Guidelines notes²¹ that appropriate safeguards may include:

- (a) provisions in contracts that address compliance with the data controller’s privacy policies and practices;

20 <www.oecd.org/sti/ieconomy/privacy-guidelines.htm> (accessed 6 April 2018).

21 *OECD Privacy Framework booklet*, available at <www.oecd.org/sti/ieconomy/privacy-guidelines.htm> at p 23 (accessed 6 April 2018).

- (b) protocols for notifying the data controller in the event of a security breach;
- (c) employee training and education;
- (d) provisions for subcontracting; and
- (e) a process for conducting audits.

27 A privacy management programme may also be demonstrated to an entity which is responsible for promoting adherence to a *code of conduct* or similar arrangement giving binding effect to the OECD Privacy Guidelines. Such arrangements may involve *seal programmes* or *certification schemes*, and may also concern transborder flows of personal data. Paragraph 21 of the OECD Privacy Guidelines encourages the *development of international arrangements* that give practical effect to the Guidelines: the Supplementary Explanatory Memorandum notes that the EU's Binding Corporate Rules ("BCRs") and the APEC CBPR system provide two models for developing such an arrangement.

28 Paragraph 16 of the 2013 version of the OECD Privacy Guidelines states the basic principle of accountability in the specific context of transborder data flows, stating that a data controller remains accountable for personal data under its control without regard to the location of the data. Paragraph 18 states that any restrictions imposed by Member countries upon transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing. In discharging the accountability principle, a data controller should assess and manage risks. Some data flows may require particular controls and safeguards because of the sensitivity of the data or because the receiving jurisdiction may lack either the willingness or capacity to enforce privacy safeguards.

29 Paragraph 17 of the 2013 version of the OECD Privacy Guidelines specifies two circumstances in which an OECD Member country should refrain from imposing restrictions on transborder flows of personal data:

- (a) Paragraph 17(a) retains the general approach from the 1980 Guidelines, by providing that Member countries should refrain from restricting transborder data flows between itself and another country where "the other country substantially observes these Guidelines".

- (b) Paragraph 17(b) provides that Member countries should refrain from restricting transborder data flows between itself and another country where “sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines”. Measures include technical and organisational security safeguards, contractual restrictions, complaint handling processes, conduct of audits, *etc.* Measures provided by the data controller taken as a whole must be sufficient and supplemented by mechanisms that ensure effective enforcement in the event these measures prove ineffective. Enforcement mechanisms may take a variety of forms, including for example, administrative and judicial oversight, as well as cross-border co-operation among privacy enforcement authorities.

30 Paragraphs 16 and 17 operate independently. The existence or absence of country restrictions on data flows adopted pursuant to paragraph 17 does not, as such, affect the operation of the principle embodied by paragraph 16, namely, that data controllers remain accountable for personal data under their control, including in the context of transborder flows.

31 The operation of the “accountability principle” and “accountability liability” in the federal Privacy Act, as we will consider further down, roughly follows paragraphs 16 and 17(b) of the 2013 version of the OECD Privacy Guidelines. In outline, APP 8.1 requires an APP entity disclosing personal information to a transborder recipient to take reasonable steps to ensure that the recipient complies with the APPs, and pursuant to section 16C the APP entity will remain accountable if the transborder recipient breaches the APPs. Consistently with paragraph 17(a) of the OECD Privacy Guidelines, Australia (as an OECD Member country) refrains from restricting transborder flows of personal data between itself and another country where the other country substantially observes the OECD Privacy Guidelines: APP 8.2(a) creates an exception from the requirements of APP 8.1 where the recipient is subject to a law or binding scheme with substantially similar protection and enforcement mechanisms. Consistently with paragraph 17(b) of the OECD Privacy Guidelines, Australia refrains from regulation of a

transborder data flow where, through compliance with APP 8.1 and section 16C, a data controller ensures that sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with the OECD Privacy Guidelines.

v *Data flows under state and territory statutes*

32 In addition to the federal Privacy Act, state and territory data privacy statutes regulate the collection and handling (use, storage and disclosure) of personal information by Australian state and territory government agencies, local (city municipal and regional) government agencies, private sector organisations providing services to those government agencies (to the extent that they handle personal information on behalf of those authorities), and in some states and territories the handling of health information by non-government health service providers and those providers' subcontractors. Victoria, NSW, Queensland, Tasmania, the ACT and the Northern Territory have legislation containing information privacy principles ("IPPs") that govern the collection and handling of personal information by state government organisations and private sector organisations that provide services on their behalf. In South Australia there is a non-legislative administrative scheme. Western Australia does not have a public sector information privacy regime.

33 Depending upon their date of enactment or relevant revisions, the state and territory statutes that generally address transborder data flows either reflect the 1980 version of the OECD Privacy Guidelines or the 2013 version of the OECD Privacy Guidelines. None of these statutes generally preclude cross-border data flows. Some statutes impose requirements for cross-border data flows in relation to government agencies and health service providers regulated by those statutes that are materially different from the requirements imposed by the federal Privacy Act in relation to APP entities disclosing personal information across borders. For example, section 33(d) of the Information Privacy Act 2009

(Qld) regulates cross-border transfers in terms that are broadly similar but different in material respects to APP 8 of the federal Privacy Act.²²

vi *Restrictions on cross-border data transfers in specific federal statutes and regulations*

34 Part IIIA of the Privacy Act regulates the Australian credit reporting system and imposes specific restrictions on the disclosure of personal “credit eligibility information” to entities that do not have an Australian link. These rules are more restrictive than those that relate to the cross-border disclosure of general personal information under APP 8, as they seek to limit disclosures of credit eligibility information to certain categories of recipients, namely, related bodies corporate of the credit provider, its credit managers and debt collectors. The Privacy Act also expressly requires the credit provider to take reasonable steps to limit the recipient’s use and disclosure of the credit eligibility information, and to ensure the recipient’s compliance with certain, but not all, APPs. An accountability principle, and corresponding accountability liability in similar terms to the provisions under section 16C of the Privacy Act, also apply to the credit provider in respect of any breaches by the recipient in relation to the information.

35 Particular government agencies and authorities are subject to additional requirements and restrictions that arise under government policy and associated administrative requirements. The most relevant federal policy guides are the current Australian Government Cloud Computing Policy,²³ and the Australian Signals Directorate guidance on cloud computing.²⁴

22 <<https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/transferring-personal-information-out-of-australia/sending-personal-information-out-of-australia>> (accessed 6 April 2018).

23 <<https://www.dta.gov.au/files/Australian%20Government%20Cloud%20Computing%20Policy%203.0-WCAG.pdf>> (accessed 6 April 2018).

24 <<https://www.asd.gov.au/infosec/cloudsecurity.htm>> (accessed 6 April 2018).

36 The relevant federal body generally administering relevant Australian government procurement, the Digital Transformation Agency (“DTA”), states:²⁵

The current Australian Government Cloud Computing Policy requires agencies to use cloud solutions where possible – when they are fit for purpose, offer the best value for money and adequately manage risk. The policy document outlines the goals and actions of the policy, the Australian Government’s definition of cloud computing, and related policies, standards and guidance. The DTA will be working in partnership with government agencies and with commercial providers to develop a Secure Cloud Strategy that will replace the 2014 policy, and make it easier for government to start using cloud technologies. The strategy will look at the challenges and options available for agencies moving to cloud solutions. We’re currently in the discovery phase of the project. It is expected the strategy will be finalised in late 2017.

37 Some private sector organisations, notably including financial services providers regulated by the Australian Prudential Regulatory Authority, are subject to additional requirements as arise under licences and prudential regulatory guides and instruments in relation to data collected and handled in the course of their regulated activities. Relevant instruments include:

- (a) Australian Prudential Regulatory Authority, Prudential Standard CPS 231: Outsourcing, July 2017, and related standards SPS 231 and HPS 231;²⁶ and
- (b) Australian Securities and Investments Commission Regulatory Guide 104, Licensing: Meeting the general obligations, a guide for Australian financial services (AFS) licensees and licence applicants.²⁷

38 Due to the sensitive nature of personal health information, the Australian health sector is subject to additional and specific statutory

25 <<https://www.dta.gov.au/what-we-do/policies-and-programs/secure-cloud/>> (accessed 6 April 2018).

26 <[www.apra.gov.au/CrossIndustry/Documents/Prudential-Standard-CPS-231-Outsourcing-\(July-2017\).pdf](http://www.apra.gov.au/CrossIndustry/Documents/Prudential-Standard-CPS-231-Outsourcing-(July-2017).pdf)> (accessed 6 April 2018).

27 <<http://download.asic.gov.au/media/3278615/rg104-published-1-july-2015.pdf>> (accessed 6 April 2018).

restrictions in relation to data protection, including My Health Records Act 2012, My Health Records Rule 2016 and My Health Records Regulation 2012, which together create the legislative framework for the Australian government's My Health Record system.²⁸

39 The My Health Records Act limits when and how health information included in a My Health Record can be collected, used and disclosed. Unauthorised collection, use or disclosure of My Health Record information is both a breach of the My Health Records Act and an interference with privacy. The OAIC regulates the handling of personal information under the My Health Record system by individuals, Australian government agencies, private sector organisations and some state and territory agencies (in particular circumstances).

40 The Healthcare Identifiers Act 2010 (Cth) regulates (among other things) the use and disclosure of healthcare identifiers.

41 State and territory health information protection Acts in some states and territories operate concurrently with the federal Privacy Act in relation to handling of health information that is personal health information by health services and providers of services to those health service providers. The Health Records Act 2001 (Vic), the Health Records and Information Privacy Act 2002 (NSW) and the Health Records (Privacy and Access) Act 1997 (ACT) govern the handling of health information in both the public and private sectors in Victoria, NSW and the ACT respectively.

42 The telecommunications sector is also subject to additional and specific statutory restrictions under:

- (a) Part 13 of the Telecommunications Act 1997 (Cth), which imposes restrictions on the use and disclosure of telecommunications and communications-related data;
- (b) Telecommunications (Interception and Access) Act 1979 (Cth), which among other things, regulates the interception of, and access to, the content of communications transiting

28 <<https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/content/home>> (accessed 6 April 2018).

telecommunications networks and stored communications (eg, SMS and e-mails) on carrier networks with enforcement agencies. This Act also includes the new data retention scheme which requires telecommunications carriers and Internet service providers to retain certain telecommunications data;

- (c) mandatory industry codes of practice administered by the Australian Communications and Media Authority and governing (among other things) telecommunications data relating to consumers; and
- (d) state and territory telecommunications interception laws.

C DATA LOCALISATION

43 There are no general data localisation requirements of general application or operation in relation to personal information in Australia.

44 As just mentioned, there are requirements for telecommunications service providers providing services within Australia or to and from Australia to provide a point of interception content delivery capability within Australia to facilitate execution of telecommunications service interception warrants issued by relevant judicial officers at the request of Australian law enforcement agencies. The relevant data may be collected or held outside Australia provided that the delivery capability is provisioned in Australia.

45 Certain categories of government-generated data (for example, sensitive information as to government-in-confidence deliberations and defence and intelligence information) are subject to particular rules that preclude that data being held outside Australia.

46 Particular rules apply to consumer credit information and some limited categories of health information and preclude that data being held outside Australia, as already mentioned earlier. For instance, the legislative framework for the Australian government's My Health Record system prevents certain My Health Record operators and service providers from holding, taking, processing or handling records held for My Health Record purposes outside Australia, and from causing or permitting anyone else to do so.

D DEFAULT POSITION, EXTRATERRITORIAL APPLICATION AND SCOPE OF APP 8

i “Accountability principle” as default rule on international data transfers

47 Generally, the federal Privacy Act does not prevent an APP entity from storing or processing personal information outside Australia, either by itself or through a third-party service provider. Before disclosing personal information to an overseas recipient, APP 8.1 requires an APP entity to take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to that information. This so-called “accountability principle” will apply where APP 8.1 applies to the disclosure, and the overseas recipient is not subject to the APPs, but the act or practice would be a breach of the APPs if it were.

48 In some circumstances, section 16C of the federal Privacy Act operates such that an act done, or a practice engaged in, by the overseas recipient that would breach the APPs if that overseas recipient was itself regulated by the APPs, is taken to be a breach of the APPs by the disclosing APP entity. The disclosing APP entity will then be legally responsible for that breach. Liability under section 16C is referred to as “accountability liability” in this report, because (in this reporter’s view) this provision imposes liability upon the disclosing AAP entity for failure to give effect to the accountability principle.

49 The intent of the accountability principle and accountability liability scheme is to provide legal incentives for a collecting and disclosing APP entity (in EU terms, a data controller) to manage “end-to-end” privacy (including information security) risks in personal information that it collects and handles: that is, to exercise the same legal responsibility as applied to its own acts and omissions in relation to acts and omissions of other entities within the data ecosystem that it creates (*ie*, subcontractors and outsourced service providers) where these entities were outside Australia and not APP entities directly regulated by the federal Privacy Act. By contractual provisions agreed with a relevant offshore subcontractor or outsourced service provider, an APP entity may agree as to the contractual distribution of liabilities arising from an act or omission of the offshore provider for which the disclosing APP entity is legally responsible. However, legal liability pursuant to section 16C of

the federal Privacy Act remains with the APP entity that discloses relevant personal information, not the relevant offshore subcontractor or outsourced service provider that was responsible for the relevant act or omission (but outside the operation of the APPs).

50 The Australian Privacy Commissioner has expressed the view that even where an APP entity takes reasonable steps to comply with APP 8, that APP entity may still be accountable under section 16C where the overseas recipient subsequently does an act or practice that would breach the APPs: see in particular “APP Guidelines, Chapter 8: APP 8 — Cross-border Disclosure of Personal Information”,²⁹ and “Privacy Business Resource 8: Sending Personal Information Overseas”.³⁰ In other words, the Australian Privacy Commissioner takes the view that even where an APP entity discharges its obligation under APP 8.1 to take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs, if the overseas recipient is responsible for an act or omission contrary to an APP and notwithstanding the APP entity that is the discloser having taken such steps as are reasonable in the circumstances, the APP entity is itself liable under section 16C. Perhaps conscious that the above expressed view of operation of section 16C imposes an onerous obligation upon contractors, the Commissioner has also stated that “when resolving matters brought to its attention under s 16C, the OAIC will take account of the reasonable steps taken by the entity to comply with APP 8.1. The OAIC’s Privacy regulatory action policy outlines a range of other matters that the OAIC will take into account in deciding when to take privacy regulatory action, and what action to take”.³¹ The Commissioner’s view as to imposition of liability remains a contestable (and thus far not judicially considered) interpretation of section 16C.

29 <<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information>> (accessed 6 April 2018).

30 <<https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-8>> (accessed 6 April 2018).

31 <<https://www.oaic.gov.au/resources/agencies-and-organisations/business-resources/privacy-business-resource-8.pdf>> (accessed 6 April 2018). The OAIC “Guide to privacy regulatory action” is available at <<https://www.oaic.gov.au/resources/about-us/our-regulatory-approach/guide-to-oaic-s-privacy-regulatory-action/oaic-regulatory-action-guide.pdf>> (accessed 6 April 2018).

ii *Extraterritorial application of federal Privacy Act (section 5B)*

51 The federal Privacy Act has extraterritorial reach. In particular, section 5B of the Privacy Act uses a concept of “Australian link” to specify a number of circumstances where, through place of incorporation or business of an entity or place from which personal information is collected or held, the Privacy Act has extraterritorial effect. An organisation or small business operator has an Australian link where it is an Australian citizen or a person whose continued presence in Australia is not subject to a legal time limitation, a partnership formed, or a trust created, in Australia or an external territory, a body corporate incorporated in Australia or an external territory, or an unincorporated association that has its central management and control in Australia or an external territory (section 5B(2)). An organisation that does not fall within one of those categories will also have an Australian link where it carries on business in Australia or an external territory, and it collected or held personal information in Australia or an external territory, either before or at the time of the act or practice (section 5B(3)).

52 The operation of the Privacy Act is generally tied to the status of the entity engaging in a particular act or practice, and the location in which an entity engages in that act or practice. Individuals whose personal information is protected by the Privacy Act need not be Australian citizens or Australian residents. For example, where an APP entity is regulated in relation to its acts or practices outside Australia (generally where it is a business established or incorporated in Australia or it is an Australian (federal) government agency), those acts or practices must conform with the requirements of the Privacy Act, regardless of requirements of local law in the jurisdiction where the act or practice occurs. Generally, compliance with local law in a foreign country where the act or practice occurs, including pursuant to any law of that foreign country, does not excuse non-compliance by an APP entity with the Privacy Act. However, an act or practice outside Australia will not breach the APPs if the act or practice is both engaged in outside Australia and required by an applicable law of a foreign country.

53 Each entity within a corporate group is generally considered separately, although related bodies corporate are treated together for limited purposes. There is no corresponding concept to EU

jurisprudence of treating corporate groups as a single enterprise, except in the limited circumstance (pursuant to section 13B) where appropriate disclosures and subsequent uses of personal information within the terms of a privacy statement and privacy notice as published by an entity within a corporate group apply in relation to uses and disclosures by all entities within that corporate group.

54 The Privacy Act also regulates as an APP entity a business outside Australia if that entity carries on a business in Australia and the relevant personal information was collected or held by the organisation or operator in Australia or an external territory, either before or at the time of the act or practice. The Australian Privacy Commissioner notes:³²

Personal information is collected ‘in Australia’ under s 5B(3)(c), if it is collected from an individual who is physically present in Australia or an external Territory, regardless of where the collecting entity is located or incorporated. An example is the collection of personal information from an individual who is physically located in Australia or an external Territory, via a website that is hosted outside Australia. This applies even if the website is owned by a company that is located outside of Australia or that is not incorporated in Australia.

Such entities are relevantly regulated only in relation to personal information collected or held by the organisation or operator in Australia or an external territory, and not other personal information handled by such entities.

iii *Type of organisations covered by APP 8*

55 “Accountability liability” (as described in this report) pursuant to section 16C of the federal Privacy Act applies if:

- (a) an APP entity discloses personal information about an individual to an overseas recipient; and

32 Office of the Australian Information Commissioner, “Australian Privacy Principles Guidelines” (available at <<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts>> (accessed 6 April 2018)) (hereinafter “APP Guidelines”) at para B.22.

- (b) Australian Privacy Principle 8.1 applies to the disclosure of the information; and
- (c) the Australian Privacy Principles do not apply, under this Act, to an act done, or a practice engaged in, by the overseas recipient in relation to the information; and
- (d) the overseas recipient does an act, or engages in a practice, in relation to the information that would be a breach of the Australian Privacy Principles (other than Australian Privacy Principle 1) if those Australian Privacy Principles so applied to that act or practice.

Accordingly, if an entity is not regulated as an APP entity, APP 8.1 will not apply to the disclosure of the information and the accountability principle will not apply to the data collector even if the relevant data are collected within Australia and disclosed to an overseas recipient.

56 A “small business operator” will be deemed to be an APP entity, and therefore required to comply with the federal Privacy Act, if that operator:

- (a) operates a business, or together with related entities related through ownership or control operate a number of businesses, with a global aggregated turnover of \$3m or more;
- (b) provides a health service or otherwise holds health information (other than in an employee record);
- (c) discloses, or collects, personal information about another individual for a benefit, service or advantage;
- (d) is a contracted service provider for a Commonwealth contract; or
- (e) is a credit reporting body.³³

57 Section 6D of the Privacy Act is the complex provision setting the criteria by which a business qualifies as a small business operator. In 2008, the Australian Law Reform Commission recommended that the small business exemption under the federal Privacy Act be removed, noting that a large number of stakeholders supported the ALRC’s

33 Privacy Act 1988 (Cth) s 6E.

proposal.³⁴ Arguments in favour of its removal were that the exemption causes regulatory inconsistency and fragmentation, hence contributes to the complexity of the privacy regime, and that the exemption was one of the major obstacles to Australia's privacy laws being recognised as "adequate" by the EU, which arguably impeded trade with the EU. The then federal government did not accept this recommendation when proposing the 2014 reforms to the Privacy Act which otherwise implemented many of the ALRC's recommendations.

iv *Type of data covered by APP 8*

58 The Privacy Act defines personal information as "information or an opinion about an identified individual, or an individual who is reasonably identifiable, (a) whether the information is true or not, and (b) whether the information is recorded in a material form or not".³⁵ Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details and commentary or opinion about a person.³⁶ A number of exceptions and exemptions apply, notably including an exemption in relation to employee records held by an organisation and relating to a current or former employment relationship between the employer and the individual.³⁷

59 Information does not have to be explicitly recognised as personal information to constitute personal information under the Privacy Act. The types of information that are personal information are unlimited.

60 The definition of personal information is not limited to information about an individual's private or family life, but extends to any information or opinion that is about the individual, from which they are reasonably identifiable. This can include information about an individual's business or work activities.

34 <<https://www.alrc.gov.au/publications/39.%20Small%20Business%20Exemption/arguments-removing-exemption>> (accessed 6 April 2018).

35 Privacy Act 1988 (Cth) s 6 (definition of "personal information").

36 <<https://www.oaic.gov.au/privacy-law/privacy-act/>> (accessed 6 April 2018).

37 Privacy Act 1988 (Cth) s 7B(3).

61 Personal information can range from sensitive and confidential information to information that is publicly available.

62 The law applies both to personal information collected in Australia, or held in Australia, without reference to the residency or citizenship of the affected individual or the country of origin of the relevant personal information.³⁸

63 There is no special treatment of “data in transit” or “outsourcing exemption”.

64 The state and territory data privacy statutes generally adopt a similar definition or interpret the varying definitions of “personal information” in the relevant statutes in a broadly similar way to the interpretation of the Australian Privacy Commissioner as discussed below (as that interpretation was revised following the seminal decision of the Full Federal Court of Australia in *Privacy Commissioner v Telstra Corp Ltd*).³⁹

65 The Australian data privacy statutes generally do not define or distinguish anonymised, pseudonymised, or encrypted data or exclude such categories from the scope of application of the law. However, a guide – “De-identification and the Privacy Act” – released by the OAIC in March 2018 expressly recognises that “[i]nformation that has undergone an appropriate and robust de-identification process is not personal information, and is therefore not subject to the Privacy Act 1988 (Cth) (Privacy Act)”.⁴⁰ Furthermore, APP 2 (anonymity and

38 The fact that the protection offered by National Privacy Principles 9 applied equally to the personal information of Australians and non-Australians was clarified by amendment to the Privacy Act 1988 (Cth) in April 2004 as part of the process of moving towards EU adequacy (see <https://www.alrc.gov.au/publications/31.%20Cross-border%20Data%20Flows%20international-privacy-protection#_ftn31> (accessed 6 April 2018)).

39 [2017] FCAFC 4 (19 January 2017); see the Office of the Australian Information Commissioner press statement: <<https://www.oaic.gov.au/media-and-speeches/statements/privacy-commissioner-v-telstra-corporation-limited-federal-court-decision>> (accessed 6 April 2018).

40 <<https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information>> (accessed 6 April 2018).

pseudonymity) provides that “[i]ndividuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter”. This does not apply if the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves, or it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

66 The key question of whether an individual that is not expressly identified is “reasonably identifiable” requires analysis of the relevant context in which the information is being handled. Certain information may be unique to a particular individual, and therefore may (in and of itself) establish a link to the particular person. However, for an individual to be “identifiable”, they do not necessarily need to be identified from the specific information being handled. An individual can be “identifiable” where the information is able to be linked (whether by the entity collecting and holding that information, or any entity to which or whom that information may be disclosed) with other information that could ultimately identify the individual. Accordingly, the circumstances in which information is held, and limitations and safeguards as to linking or disclosure of that information, are relevant circumstances to be taken into account in determining whether an entity holds or discloses personal information.

67 The inclusion of the term “reasonably” in the definition of personal information means that where it is possible to identify an individual from available information, the next consideration is whether, objectively speaking, it is reasonable to expect that the subject of the information could be identified. Even though it may be technically possible to identify an individual from information, if doing so is so impractical that there is almost no likelihood of it occurring, the information would not generally be regarded as “personal information”. In this respect, the OAIC guide, “De-identification and the Privacy Act” prescribes that de-identification not only requires “the removal of direct identifiers”, but also “taking one or both of the following additional steps: – the removal or alteration of other information that could potentially be used to re-identify an individual, and/or – the use of controls and safeguards in the data access environment to prevent re-identification”.

68 See further OAIC, “De-identification and the Privacy Act”;⁴¹ “What is Personal Information?”;⁴² OAIC and CSIRO’s Data61, “De-identification Decision-Making Framework”;⁴³ and the Information and Privacy Commission, NSW, “Fact Sheet: Reasonably Ascertainable Identity”.⁴⁴

E LEGAL BASES UNDER FEDERAL PRIVACY ACT AND APP 8

i *Exceptions to accountability principle in APP 8.2 – Overview*

69 APP 8.2 lists a number of exceptions to APP 8.1 (and therefore to the operation of the accountability principle in section 16C). Relevantly, APP 8.1 will not apply where:

- (a) the entity reasonably believes that the recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that is, overall, substantially similar to the APPs; and there are mechanisms available to the individual to enforce that protection or scheme (APP 8.2(a)) (see further below);
- (b) an individual consents to the cross-border disclosure, after the entity informs them that APP 8.1 will no longer apply if they give their consent (APP 8.2(b));
- (c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order (APP 8.2(c));
- (d) the disclosure of the information is because one of a limited list of “permitted general situations” (*per* sub-section 16A(1) of the federal Privacy Act) exist in relation to the disclosure of the information by the APP entity – in particular, it is unreasonable or impracticable to obtain an individual’s consent and the entity

41 <<https://oaic.gov.au/agencies-and-organisations/guides/de-identification-and-the-privacy-act>> (accessed 6 April 2018).

42 <<https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information>> (accessed 6 April 2018).

43 <<https://www.oaic.gov.au/agencies-and-organisations/guides/de-identification-decision-making-framework>> (accessed 6 April 2018).

44 <<https://www.ipc.nsw.gov.au/fact-sheet-reasonably-ascertainable-identity-0>> (accessed 6 April 2018).

reasonably believes that the relevant disclosure is necessary to prevent or lessen a serious threat to the life, health or safety of any individual, or to public health and safety, or the entity has reason to suspect unlawful activity or misconduct of a serious nature that relates to the entity's functions or activities and the entity reasonably believes that the disclosure is necessary in order for the entity to take appropriate action, or the disclosure is to locate a person reported as missing (subject to any rules prescribed by the Privacy Commissioner pursuant to section 16A(2)) (APP 8.2(d));

- (e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party (APP 8.2(e)); and
- (f) the entity is a government agency, and (both) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body, and the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body (APP 8.2(f)).

ii *Distinction between “use” and “disclosure”*

70 A transfer of personal information to an overseas recipient may not be a “disclosure” regulated by APP 8 if the personal information at all times remains under the effective control of the APP entity. The Australian Privacy Commissioner has drawn a distinction between limited and controlled access to information by an overseas recipient under conditions prescribed by the APP entity, which may in appropriate circumstances be a “use” by the APP entity rather than a “disclosure” to an overseas entity. This distinction will be important in relation to many outsourcing and offshoring arrangements, including cloud service or “as-a-service” offerings.

71 In relation to “disclosure”, the APP Guidelines state:

B.64 An APP entity discloses personal information when it makes it accessible or visible to others outside the entity and releases the

subsequent handling of the personal information from its effective control. This focuses on the act done by the disclosing party, and not on the actions or knowledge of the recipient. Disclosure, in the context of the Privacy Act, can occur even where the personal information is already known to the recipient.

B.65 The release may be a proactive release, a release in response to a specific request, an accidental release or an unauthorised release by an employee.

The APP Guidelines provide various examples (B.65).

72 The APP Guidelines, furthermore, state that “[w]here an APP entity engages a contractor to perform services on its behalf, the provision of personal information to that contractor will in most circumstances be a disclosure” (B.67). However, the APP Guidelines also state:

B.144 In limited circumstances, providing personal information to a contractor to perform services on behalf of the APP entity may be a use, rather than a disclosure (see paragraph B.63–B.68). This occurs where the entity does not release the subsequent handling of personal information from its effective control. For example, if an entity provides personal information to a cloud service provider for the limited purpose of performing the services of storing and ensuring the entity may access the personal information, this may be a ‘use’ by the entity in the following circumstances:

- a binding contract between the entity and the provider requires the provider only to handle the personal information for these limited purposes
- the contract requires any subcontractors to agree to the same obligations, and
- the contract gives the entity effective control of how the information is handled by the provider. Issues to consider include whether the entity retains the right or power to access, change or retrieve the information, who else will be able to access the information and for what purposes, the security measures that will be used for the storage and management of the personal information and whether the information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract.

iii *Duties of APP entities in case of “disclosure”*

73 Where there is a disclosure and APP 8 operates, the Australian Privacy Commissioner suggests⁴⁵ that enforceable contractual arrangements should specify:

- (a) obligations substantively similar to the APPs (other than APP 1);
- (b) the purpose/s for which the overseas recipient and any subcontractors are permitted to use or disclose the personal information — noting that APP 6 outlines when an APP entity may use or disclose personal information;
- (c) the minimum technical and organisational measures that will apply to ensure the security of the personal information overseas — noting that APP 11 requires an APP entity to take active measures to ensure the security of personal information it holds;
- (d) agreed procedures for providing access to personal information on request, and for making any necessary corrections — noting that APPs 12 and 13 require an APP entity to give access to, and correct, an individual’s personal information in certain circumstances;
- (e) a requirement that the recipient implement a data breach response plan which includes a mechanism for notifying the APP entity where there are reasonable grounds to suspect a data breach and outlines appropriate remedial action (based on the type of personal information to be handled under the contract); and
- (f) mechanisms that enable the APP entity to monitor compliance with these arrangements.

74 The law or OAIC guidance do not specify if the contract must contain a third-party beneficiary clause to the benefit of the individual whose data are transferred. In general, a right for an individual to enforce a contractual right through an ability to institute legal proceedings is

45 APP Guidelines, Chapter 8: APP 8 — Cross-border disclosure of personal information (<<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information>> (accessed 6 April 2018)), in particular at paras 8.12–8.18.

unlikely to be regarded as an effective enforcement mechanism as envisaged by the exception in APP 8.2(a).⁴⁶

75 The Australian Privacy Commissioner further suggests that the contractor should ensure that non-contractual mechanisms are in place that minimise the risk that personal information will be mishandled by the overseas recipient, for example by:

- (a) verifying that the overseas recipient has in place technical and organisational safeguards (such as security policies and procedures, staff training in personal information security, access restrictions and audit controls) to ensure that the personal information is secure to the standard required under APP 11; and
- (b) asking the recipient to provide the APP entity with any internal policies and procedures for handling personal information, such as privacy policies, information-security policies and data retention policies, and checking these provide for practices that are generally equivalent to the APP requirements.

76 Many APP entities endeavour to give effect to the accountability principle in APP 8.1 and follow the Australian Privacy Commissioner's guidance as to contractual and extra-contractual "reasonable steps" to be taken before disclosing personal information to an overseas recipient.

77 In considering the distinction between "use" and "disclosure", it is important to not overstate the significance of that distinction when applying a privacy risk management. As stated by the Australian Privacy Commissioner:⁴⁷

[T]he OAIC recognises that in some instances, it can be difficult to determine whether the information is being 'used', or whether it is being 'disclosed'. In such cases, the practical effect of distinguishing a 'use' from a 'disclosure' should not be overstated. Whether an APP entity sends personal information to an overseas recipient as a 'use' or as a 'disclosure', it may still be held accountable for mishandling of that information by the

46 APP Guidelines at paras 8.25–8.26.

47 <<https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-8>> (accessed 6 April 2018).

overseas recipient. In practice, the steps that an APP entity takes and their accountability when sending personal information overseas can be similar regardless of whether the information is being used or disclosed. For this reason, where it is unclear whether the personal information is being used or disclosed, the best approach is to take reasonable steps to ensure the APP are complied with. An APP entity that sends personal information overseas may be liable if the personal information is mishandled.

78 This area of regulation is still developing and care should be taken to review and follow OAIC guidance. See in particular “APP Guidelines, Chapter 8: APP 8 — Cross-border Disclosure of Personal Information”;⁴⁸ and “Privacy Business Resource 8: Sending Personal Information Overseas”.⁴⁹

79 In addition, a Notifiable Data Breaches (“NDB”) scheme will operate in Australia from 22 February 2018, pursuant to amendments to the Privacy Act which enter into operation in relation to eligible data breaches that occur on, or after, that date. The NDB scheme requires organisations covered by the Privacy Act to notify any individuals likely to be at risk of serious harm by a data breach. If an APP entity discloses personal information to an overseas recipient that is not regulated as an APP entity, in line with the requirements of APP 8, then the APP entity is deemed to “hold” the information for the purposes of the NDB scheme. The practical effect is that if personal information held by the overseas recipient is subject to unauthorised access or disclosure, the APP entity is still responsible for assessing whether it is an eligible data breach under the Privacy Act, and if it is, for notifying the Commissioner and individuals at risk of serious harm.

iv Consent

80 Consent is available as an exception under APP 8.1 disclosure. The requirements for valid informed consent are relatively prescriptive,

48 <<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information>> (accessed 6 April 2018).

49 <<https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-8>> (accessed 6 April 2018).

although an active expression of consent (active opt-in) is not required. In fact, the requirement that consent is obtained “after the entity informs them that APP 8.1 will no longer apply if they give their consent” imposes a significant practical burden, both in terms of prominence and clarity of statement required to discharge this requirement.⁵⁰ Although it is not uncommon to include a statement in a privacy policy and in a privacy notice which might be argued to comply with the requirement in APP 8.2(b), many APP entities also take steps to comply with APP 8.1. In other words, few APP entities appear to take the legal and reputational risks attendant upon assessing that a purported consent under APP 8.2(b) avoids operation of the requirement to discharge the accountability principle in APP 8.1.

81 The APP Guidelines⁵¹ provide guidance on consent under APP 8 as follows:

- 8.28 An APP entity should provide the individual with a clear written or oral statement explaining the potential consequences of providing consent. At a minimum, this statement should explain that if the individual consents to the disclosure and the overseas recipient handles the personal information in breach of the APPs:
- the entity will not be accountable under the Privacy Act
 - the individual will not be able to seek redress under the Privacy Act.
- 8.29 The statement should also:
- be made at the time consent is sought
 - not rely on assumed prior knowledge of the individual.
- 8.30 The statement could also explain any other practical effects or risks associated with the disclosure that the APP entity is aware of, or would be reasonably expected to be aware of. These may include that:
- the overseas recipient may not be subject to any privacy obligations or to any principles similar to the APPs
 - the individual may not be able to seek redress in the overseas jurisdiction

50 APP Guidelines at paras 8.27–8.33.

51 APP Guidelines at paras 8.28–8.33.

- the overseas recipient is subject to a foreign law that could compel the disclosure of personal information to a third party, such as an overseas authority.
- 8.31 Consent is defined in s 6(1) as ‘express consent or implied consent’, and is discussed in more detail in Chapter B (Key concepts). The four key elements of consent are:
- the individual is adequately informed before giving consent (in this case ‘expressly informed’)
 - the individual gives consent voluntarily
 - the consent is current and specific, and
 - the individual has the capacity to understand and communicate their consent.
- 8.32 An APP entity does not need to obtain consent before every proposed cross-border disclosure. It may obtain an individual’s consent to disclose a particular kind of personal information to the same overseas recipient for the same purpose on multiple occasions, providing it has expressly informed the individual of the potential consequences of providing that consent. In doing this, the entity should not seek a broader consent than is necessary for its purposes, for example, consent for undefined future uses, or consent to all legitimate uses or disclosures.
- 8.33 If an individual withdraws their consent, the APP entity must no longer rely on the original consent when dealing with the individual’s personal information.

82 Given these prescriptive requirements, many privacy policies (statements) and privacy notices are quite explicit as to overseas transfers or personal information.

v Overseas recipient subject to “law or binding scheme”

83 An overseas recipient may be subject to a “law or binding scheme” under APP 8.2(a), where, for example, it is:

- (a) bound by a *privacy or data protection law* that applies in the jurisdiction of the recipient;
- (b) required to comply with *another law* that imposes obligations in relation to the handling of personal information (such as some taxation laws which expressly authorise and prohibit specified uses and disclosures and include a right of access to an individual’s personal information);

- (c) subject to an *industry scheme* or *privacy code* that is enforceable once entered into, irrespective of whether the recipient was obliged or volunteered to participate or subscribe to the scheme or code; or
- (d) subject to *Binding Corporate Rules* (“BCRs”).⁵²

84 The conditions to operation of this exception create a substantial practical burden. To fall within the exception, an entity must “reasonably believe that the recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that is, overall, substantially similar to the APPs; and there are mechanisms available to the individual to enforce that protection or scheme”.⁵³ The OAIC does not operate a “white list” that endorses disclosures to any particular foreign recipients or any specific foreign jurisdictions, so a subjective judgment by the discloser is required. The law does not list substantive standards to establish that the law of another jurisdiction or binding scheme has the effect of protecting the information in a way that is, overall, substantially similar to the APPs.

85 Further, this requirement is specific to laws or binding schemes that (in overall effect) protect personal information “in a way that is, overall, substantially similar to the APPs”. In some cases, and in particular as to many secondary uses, the requirements of the APPs are higher or more specific than the nine data privacy principles in the APEC Privacy Framework. As well, the law or binding scheme governing the recipient entity may not make “mechanisms available to the individual to enforce that protection or scheme”. Certification of an organisation’s privacy policies and practices (its CBPRs) has the effect that those CBPRs become enforceable against that organisation by the local privacy regulator or the accountability agent (“AA”). However, that enforceability may not be a mechanism available to the individual to enforce that protection or scheme. Although it is not uncommon to negotiate contractual terms between a discloser and a recipient that create a scheme of privacy protection analogous to the substantive effect of the APPs, many APP entities do so in circumstances which might be argued

52 See APP Guidelines at para 8.21.

53 See APP Guidelines at paras 8.19–8.26.

both to give effect to the accountability principle in APP 8.1 and to fall within the exception in APP 8.2(a).

86 The Australian Privacy Commissioner has to date declined to provide guidance as to adequacy of a law or binding scheme and remedies available to individuals under that law or scheme. It is likely that the Australian government's announcement of Australia's intention to participate in the APEC CBPR system will lead to the Australian Privacy Commissioner reconsidering this position.

vi CBPRs

87 As at 17 February 2018, Australia had announced its intention to participate in the APEC CBPR system but had not announced formal lodgement of a Notice of Intent. This announcement of intention followed a public consultation as to whether to participate in the APEC CBPR system.⁵⁴

88 To participate in the APEC CBPR system, organisations (including corporations) in APEC economies must develop and implement privacy policies and practices that are consistent with the APEC Privacy Framework and, in particular, the nine data privacy principles established under the Framework.⁵⁵ Organisations must then submit their policies and practices, in the form of a completed APEC-recognised CBPR questionnaire, to a locally based, APEC-recognised AA for assessment against the CBPR program requirements. If an AA determines that an organisation's policies and practices are consistent with the CBPR program requirements, the organisation is certified as CBPR compliant and its details are added to the CBPR system "white list". This then allows an organisation to represent to consumers that it

54 Consultation paper at <<https://www.ag.gov.au/Consultations/Documents/APEC-Cross-border-privacy-rules/Australia-and-the-APEC-CBPR-system-paper.DOCX>> (accessed 6 April 2018); submissions and announcement at <<https://www.ag.gov.au/Consultations/Pages/APEC-cross-border-privacy-rules-public-consultation.aspx>> (accessed 6 April 2018).

55 <[https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-\(2015\)](https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015))> (accessed 6 April 2018).

complies with data privacy standards that are recognised throughout the Asia-Pacific region. Upon certification, an organisation's privacy policies and practices – that is, its CBPRs – become enforceable against that organisation by the local privacy regulator or the AA.

89 However, an organisation's certification under the CBPR system extends only to the extent of the organisation's compliance with the CBPR program requirements. Certification does not purport to certify that the organisation is compliant with domestic data privacy regulation, which domestic requirements (of both the data originating country and the data recipient country) apply above and beyond the CBPR program requirements. Of course, domestic data privacy regulation of countries within the Asia-Pacific region takes a wide variety of forms. Accordingly, compliance with domestic privacy regulation requires country-by-country review, to be conducted in addition to the CBPR program requirements.

90 Accordingly, the requirements of Australian data privacy law apply to organisations in Australia sending (disclosing) personal information to any and all countries, including countries that participate in the APEC CBPR system. As already noted, APP 8 regulates cross-border disclosure by APP entities of personal information to recipients outside of Australia. Before disclosing personal information to an overseas recipient, APP 8.1 requires an APP entity to take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to that information. This so-called "accountability principle" will apply where APP 8.1 applies to the disclosure, and the overseas recipient is not subject to the APPs, but the act or practice would be a breach of the APPs if it were. This will be the case regardless of whether the act or practice in the recipient country was compliant with domestic data privacy laws in operation in that country and the nine data privacy principles in the APEC Privacy Framework in respect of which the organisation's compliance with the CBPR program requirements is certified by an AA. That noted, APP 8.1 requires an APP entity to take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the personal information disclosed to it.

91 One view of the operation of section 16C to impose accountability liability is that if an APP entity has made a disclosure to an entity in

circumstances where the recipient entity is certified as compliant with the CBPR program requirements and the discloser has taken reasonable steps to verify that compliance in practice, these circumstances are indicative of discharging the “accountability principle” by taking reasonable steps under APP 8.1 and accordingly accountability liability under section 16C of the federal Privacy Act should not operate. However, this view has not been tested by litigation and has not been supported by regulatory guidance by the Australian Privacy Commissioner. Accordingly, there remains a strong view that an APP entity must specifically discharge requirements in the exceptions to APP 8.1 in order to have taken reasonable steps under APP 8.1 and to avoid accountability liability under section 16C.

92 Most relevantly, APP 8.1 will not apply where an entity reasonably believes that the recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that is, overall, substantially similar to the APPs; and there are mechanisms available to the individual to enforce that protection or scheme (APP 8.2(a)). This requirement is specific to laws or binding schemes that (in overall effect) protect personal information “in a way that is, overall, substantially similar to the APPs”. In some cases, and in particular as to many secondary uses, the requirements of the APPs are higher or more specific than the nine data privacy principles in the APEC Privacy Framework. Further, the law or binding scheme governing the recipient entity may not make “mechanisms available to the individual to enforce that protection or scheme”. Certification of an organisation’s privacy policies and practices (its CBPRs) has the effect that those CBPRs become enforceable against that organisation by the local privacy regulator or the AA. However, that enforceability may not be a mechanism available *to the individual* to enforce that protection or scheme.

93 The Attorney-General’s Department’s consultation paper entitled “Australia and the APEC Cross-Border Privacy Rules (CBPR) System”⁵⁶ directly addressed these views, as follows:

56 <<https://www.ag.gov.au/Consultations/Pages/APEC-cross-border-privacy-rules-public-consultation.aspx>> (accessed 6 April 2018).

Is CBPR a 'binding scheme' that is 'overall, at least substantially similar' to the APPs? The inclusion of the phrase 'binding scheme' in APP 8.2 was specifically intended to capture possible future arrangements, such as if Australia were to participate in the APEC CBPR system, but only if these arrangements meet the criteria of being 'at least substantially similar' to the APPs. As said, neither the department nor the OAIC operate a 'white list' that endorses disclosures to any particular foreign recipients or any specific foreign jurisdictions. However, Australian participation in the CBPR system would provide a basis for APP entities to assume that disclosure to a foreign recipient that is subject to a CBPR compliant Accountability Agent in another jurisdiction was subject to a binding scheme that was, overall, 'substantially similar' to the APPs.

Are there mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme? The wording of APP 8.2 was also specifically designed to provide flexibility for future enforcement arrangements. The Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 stated that: 'It is not essential that the overseas jurisdiction have an office equivalent to the OAIC in order to provide accessible enforcement mechanisms. It should be possible for a range of dispute resolution or complaint handling models to satisfy this requirement. Effective enforcement mechanisms may be expressly included in a law or binding scheme or may take effect through the operation of cross-border enforcement arrangements between the OAIC and an appropriate regulatory authority in the foreign jurisdiction.' Accordingly, the second limb of APP 8.2(a) would allow for effective enforcement mechanisms of the kind that Australia would need to arrange in any event to participate in the CBPR scheme. [T]hese mechanisms could be in the form of a binding code or a co-regulatory approach to enforce the more specific prescriptive provisions of the CBPR.

94 However, in the Commissioner's submission dated 27 July 2017 to the Australian Attorney-General made in response to that consultation paper, the Australian Privacy Commissioner stated as follows:⁵⁷

Given the increasing regional engagement in the CBPR system referred to in the consultation paper, I am particularly interested to understand

57 <<https://www.oaic.gov.au/engage-with-us/submissions/australia-and-the-apec-cross-border-privacy-rules-cbpr-system-submission-to-attorney-general-s-department>> (accessed 6 April 2018).

whether there is broad industry and community support for Australia's participation. I will also be looking to understand whether any privacy concerns raised in this consultation can be addressed by tailoring the implementation of this system to ensure consistency with Australia'[s] domestic privacy framework.

If there is support for Australia's participation, I look forward to working with AGD to ensure the CBPR system is implemented in a way that maintains and builds upon the existing privacy protections set out in the *Privacy Act 1988* (the Privacy Act), and reflects community expectations of privacy. In particular, I will be looking to ensure the CBPR system strikes a reasonable balance between facilitating the free flow of information across borders while ensuring that the privacy of individuals is respected, consistent with the objects of the Privacy Act. This would include ensuring that the system, as implemented in Australia, provides for appropriate and accessible complaint and redress mechanisms.

95 The position as at 21 March 2018 is that in the absence of any court decision or definitive regulatory statement, it remains legally unclear whether and in what circumstances verification of certification of a recipient entity as compliant with the CBPR program requirements will constitute the taking of reasonable steps under APP 8.1 such that accordingly accountability liability under section 16C of the federal Privacy Act should not operate.

vii *Certification, trustmarks and privacy seals*

96 In principle, certification mechanisms, privacy seals and trustmarks delivered in a third country could be considered as a valid means for a data exporter to demonstrate compliance with APP 8.1. This is in line with the Supplementary Explanatory Memorandum of the OECD Privacy Framework, and in fact, in 2008 the Australian Law Reform Commission noted that one feature of the APEC Privacy Framework that may have application in the Australian context was a trustmark scheme. It noted that a number of countries have already adopted trustmark schemes, including privacy trustmark schemes, which varied in nature and structure. For example, in the US, trustmark bodies are private sector organisations, whereas in Singapore, the National Trust Council's trustmark "TrustSg" is publicly supported by Singapore's Infocomm Development Authority.

97 The relevant question today would be whether the APP entity had discharged its obligation under APP 8.1 to take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the information. Certifications would be relevant to this evaluation, although it is clear that the Australian Privacy Commissioner would consider whether the relevant certifications provided adequate assurance that the overseas recipient would not breach the APPs.

98 The law could accommodate a mechanism of mutual recognition of trustmarks or privacy seals delivered in another jurisdiction through supporting guidance from the Australian Privacy Commissioner, although that guidance would remain subject to review by Australian courts as to whether it was a proper interpretation and application of the law.

viii Conclusion

99 In summary, the difficulties attendant upon reliance on the two key exceptions (consent, *per* APP 8.2(a), or “law or binding scheme”, *per* APP 8.2(b)) to the accountability principle in APP 8.1, are such that even where APP entities might reasonably suggest that they fall within either or both exceptions, more prudent and properly advised APP entities take active steps to discharge the accountability principle in APP 8.1. APP entities that actively endeavour to give effect to the accountability principle in APP 8.1 generally follow the Australian Privacy Commissioner’s guidance as to contractual and extra-contractual “reasonable steps” to be taken before disclosing personal information to an overseas recipient. However, this approach can be difficult to mesh with upstream requirements (for example, as to BCRs).

F CO-OPERATION BETWEEN OAIC AND FOREIGN PRIVACY ENFORCEMENT AUTHORITIES

100 The OAIC can investigate an alleged interference with privacy (and certain other privacy breaches), either following a complaint or on the Commissioner’s own initiative (Commissioner initiated investigation (“CII")). A complaint or CII may result in enforcement action being

taken. The Commissioner has issued a “Guide to privacy regulatory action”,⁵⁸ in which it details its enforcement policy. The OAIC is expressly empowered to entertain complaints and conduct investigations concerning extraterritorial acts and practices where there is a relevant “Australian link”: section 5B(4).

101 Australian data privacy law does not include provisions that specifically empower the PEA to develop operational co-operation with the PEAs in other jurisdictions. However, Australian regulators in most sectors actively pursue international co-operation and where appropriate, conduct joint investigations with like regulators administering comparable legislation.

102 In its Privacy Regulatory Action Policy (June 2015) (“Interaction with foreign regulators”),⁵⁹ the Australian Privacy Commissioner states:

Many privacy threats and challenges extend beyond national boundaries. A coordinated and consistent global response can be an effective regulatory response to a global privacy issue. In dealing with an interference with privacy or potential privacy risk that operates across national boundaries, there can be a practical and resource advantage in liaising with other privacy regulators to avoid duplication, share information and coordinate the release of investigation findings.

The OAIC will seek to work in partnership with privacy regulators in foreign jurisdictions where there is a shared interest in working together to address privacy breaches, threats and risks. Through such partnerships, the OAIC will share knowledge and expertise with a view to ensuring a consistent and harmonised approach to regulatory action in a particular matter. If appropriate, it may also seek to coordinate regulatory activities and share investigative information with foreign privacy regulators.

However, the OAIC will always operate independently within its legislative framework, including limits on its ability to share information. In addition, where information is shared, only necessary information will

58 <<https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/>> (accessed 6 April 2018).

59 <<https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/#working-with-other-complaint-and-regulatory-bodies>> (accessed 6 April 2018). See further <<https://www.oaic.gov.au/engage-with-us/networks>> (accessed 6 April 2018).

be shared and the information exchange will occur under an information sharing arrangement which protects the confidentiality of the information.

As part of this commitment to international cooperation and privacy enforcement, the OAIC will continue to actively engage with global privacy networks, including the Asia Pacific Privacy Authorities Forum (APPA), the OECD Global Privacy Enforcement Network (GPEN) and the APEC Cross Border Privacy Enforcement Arrangement.

103 Consistent with this approach, the Australian Privacy Commissioner can be expected to endeavour to ensure reasonable consistency wherever practicable in the application of privacy laws in order to minimise impediments to transborder commerce while maintaining standards of data protection substantially consistent with the OECD Privacy Guidelines and the Australian statute. The OAIC participates in several international forums and arrangements to:

- (a) promote best privacy practice internationally;
- (b) address emerging privacy issues in the region; and
- (c) co-operate on cross-border privacy regulation and enforcement matters.

104 By way of examples:

- (a) the OAIC has concluded a memorandum of understanding covering the management of cross-border privacy complaints, possible joint investigations and co-operation on privacy issues with the Office of the New Zealand Privacy Commissioner;⁶⁰
- (b) the OAIC submitted comments on the Office of the Privacy Commissioner of Canada's ("OPCC") Discussion Paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act ("PIPEDA");⁶¹

60 <<https://www.privacy.org.nz/assets/Files/Australia-New-Zealand-signed-Memorandum-of-Understanding-27-August-2008.pdf>> (accessed 6 April 2018).

61 <<https://www.oaic.gov.au/engage-with-us/submissions/discussion-paper-on-consent-and-privacy-submission-to-the-office-of-the-privacy-commissioner-of-canada>> (accessed 6 April 2018).

- (c) the OAIC has expressed concern to ensure consistent implementation of cyber engagement strategy by Australia and its trading partners;⁶² and
- (d) the OAIC has conducted joint investigations: see, for example, the report of the joint investigation into the Ashley Madison data breach conducted by the Australian Privacy Commissioner and the Privacy Commissioner of Canada⁶³ and the enforceable undertaking provided by Ruby Corp (then Avid Life Media).⁶⁴

105 The Australian Privacy Commissioner has also been an active participant in The Global Cross Border Enforcement Cooperation Arrangement (“GCBECA”) since its commencement in October 2015. The Australian Privacy Commissioner is an Accredited Member and active participant of the International Conference of Data Protection and Privacy Commissioners, Global Privacy Enforcement Network (“GPEN”), GPEN Alert (from inception in October 2015), ICDPPC Enforcement Cooperation Arrangement, the Unsolicited Communications Enforcement Network (“UCENet”), and APEC Cross-border Privacy Enforcement Arrangement (“CPEA”). In accordance with the CPEA, the Australian Privacy Commissioner published the Summary Statement of Privacy Enforcement Authority enforcement practices, policies and activities.⁶⁵

62 Office of the Australian Information Commissioner submission to the Department of Foreign Affairs and Trade on the International Cyber Engagement Strategy, 7 April 2017, available at <<https://www.oaic.gov.au/engage-with-us/submissions/international-cyber-engagement-strategy-submission-to-the-department-of-foreign-affairs-and-trade>> (accessed 6 April 2018).

63 <<https://www.oaic.gov.au/media-and-speeches/media-releases/ashley-madison-data-breach-joint-findings-released>> (accessed 6 April 2018).

64 <<https://www.oaic.gov.au/privacy-law/enforceable-undertakings/avid-life-media-enforceable-undertaking>> (accessed 6 April 2018).

65 Available at <<https://www.oaic.gov.au/about-us/corporate-information/mous/summary-statement-of-privacy-enforcement-authority-enforcement-practices-policies-and-activities>> (July 2014) (accessed 6 April 2018).

Jurisdictional Report

THE PEOPLE'S REPUBLIC OF CHINA

Reporter: **Kemeng Cai**
Associate, Dentons Beijing Office

A INTRODUCTION

1 Data privacy protection in China has been strengthened in recent years, with a series of regulations and national standards containing data privacy protection rules being adopted in the past decade. The Tort Liability Law (2009) adopted in 2009 for the first time expressly protects individual's right to privacy under Chinese laws, and the Seventh Amendment of the Criminal Law (2009) adopted in the same year criminalises certain illegal sale, provision, stealing or acquisition of personal information also for the first time. The Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks (2012)¹ adopted in 2012 is the first special legislation addressing personal information protection under PRC laws. Other important regulations and standards regarding data privacy protection or containing data privacy protection requirements include the Guidelines for Personal Information Protection within Public and Commercial Services Information Systems (2013),² the Provisions on Protecting the Personal Information of Telecommunications and Internet Users (2013),³ the Consumer

1 <http://www.npc.gov.cn/npc/xinwen/2012-12/29/content_1749526.htm> (accessed 26 March 2018).

2 <<http://download.csdn.net/download/wangqingahi/8433019>> (accessed 26 March 2018).

3 <http://www.gov.cn/gongbao/content/2013/content_2473881.htm> (accessed 26 March 2018).

Protection Law (2013 Revision)⁴ and the Ninth Amendment to the Criminal Law (2015).⁵

2 The Cybersecurity Law⁶ adopted by the National People's Congress Standing Committee (the legislative body of China) on 7 November 2016 is a landmark development in data privacy protection. Although the law is mainly devoted to safeguarding the "cyberspace sovereignty" of China and reinforce cybersecurity,⁷ it also contains the most comprehensive and broadly applicable data privacy protection requirements to date. Protection of personal information⁸ is a key dimension of data security (or "network information security" as used in

4 <http://www.npc.gov.cn/npc/xinwen/2013-10/26/content_1811773.htm> (accessed 26 March 2018).

5 <http://www.npc.gov.cn/npc/xinwen/2015-08/31/content_1945587.htm> (accessed 26 March 2018).

6 <http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm> (accessed 26 March 2018).

7 The new Cybersecurity Law is the first comprehensive law in China specifically regulating cybersecurity. The cybersecurity issue has been deemed by the Chinese government as a growing challenge to national security in recent years because of the increasingly vital role the Internet plays in the Chinese economy, society and politics. Concerns regarding cyberspace national security appears to have further increased since Edward Snowden's disclosures in 2013 regarding the surveillance activities of the US National Security Agency. In his response, President Xi Jinping raised the slogan "no cyber safety means no national security" in 2014 and called for protecting China's cyber sovereignty on different occasions (<http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm> (accessed 26 March 2018)). The legislative and regulatory activities of the Chinese government relating to cybersecurity protection have increased laws since 2014. A series of national security legislation adopted in recent years, such as the National Security Law (2015) (<http://www.npc.gov.cn/npc/xinwen/2015-07/07/content_1941161.htm> (accessed 26 March 2018)) and the Counter-Terrorism Law (2015), contain provisions relating to cybersecurity (<http://news.xinhuanet.com/politics/2015-12/27/c_128571798.htm> (accessed 26 March 2018)).

8 The law uses the term "personal information" rather than "data privacy" or "personal data", while the basic requirements of personal information protection embody mainstream international data privacy principles such as transparency, data quality, individual participation and purpose specification. This article uses the terms "personal information" and "data privacy" interchangeably.

the Cybersecurity Law),⁹ an inseparable component of cybersecurity under the law.

3 The personal information protection provisions¹⁰ under the Cybersecurity Law codify the requirements embodied in existing laws and regulations, and incorporate new or more explicit requirements with respect to the right to correct and delete personal information, data breach notification, transfer of personal information, and data localisation. Unlike existing data privacy laws and regulations which are largely sectoral, the data privacy protection provisions under the Cybersecurity Law broadly apply to network operators, which may encompass almost all public and private entities using a network to process information (as further elaborated below in Part C).¹¹ Most importantly and pertinent to our theme, the Cybersecurity Law provides data localisation requirements for the personal information and the so-called “important data” processed by certain critical network operators for the first time at the level of national law.

9 Chapter 4 of the Cybersecurity Law concerns “Network Information Security” (Arts 40–50), which includes provisions on protection of enterprise information and personal information and online content control. Yanqing Hong, a leader of the personal data protection project for the National Information Security Standardization Technical Committee of China (hereinafter “TC 260”), is deputy head of the task force for the Guidelines for Data Cross-Border Transfer Security Assessment. He summarises the provisions of the Cybersecurity Law on data into three levels according to their different dimensions of protection – data security, personal data protection and national-level data protection. The relationship between the three dimensions are summarised as follows:

- (a) Data security = confidentiality + integrity + availability.
- (b) Personal information protection = data security + basic principles on personal information collection and use (legality, justification, necessity, transparency, *etc*) + individual right to delete or correct.
- (c) National-level data protection = data security + control over important data + cross-border data transfer security assessment.

See Yanqing Hong, *The Cross-Border Data Flows Security Assessment: An Important Part of Protecting China’s Basic Strategic Sources*, Working Paper, 20 June 2017 <<http://apide.org/apru-asia-eu-dialogue/readings/CrossBorderDataFlows.pdf>> (accessed 26 March 2018).

10 Chapter 4 of the Cybersecurity Law, Arts 41–45.

11 See paras 20–43 below.

4 This report will provide an overview of the regulation of cross-border transfer of data from China and focus on the landmark Cybersecurity Law. It will show that such a data localisation requirement is not only driven by the demand for protection of personal information, but also, or even mainly, by national security considerations. Part B¹² will briefly introduce existing regulations on cross-border transfer of data before the enactment of the Cybersecurity Law. Part C¹³ provides a comprehensive introduction to the Cybersecurity Law and the ancillary regulations. Part D¹⁴ provides a brief analysis of the potential challenges and implications of the Cybersecurity Law.

B CROSS-BORDER TRANSFER OF DATA BEFORE THE CYBERSECURITY LAW

i *Regulations on cross-border transfer of data before the Cybersecurity Law*

5 Before the adoption of the Cybersecurity Law, regulations governing cross-border transfer of data from China were interspersed across a number of sectoral laws and regulations governing specific industries or types of data. Data subjected to localisation requirements include both personal information and data with a bearing on national security. Companies, in particular multinational companies operating in China, usually encounter regulatory restrictions for cross-border transfer of data in the following cases.

a State secrets

6 The strictest restrictions on the transfer of data come from various laws and regulations protecting state secrets, in particular the Law on the Protection of State Secrets of the People's Republic of China,¹⁵ the

12 See paras 5–19 below.

13 See paras 20–43 below.

14 See paras 44–50 below.

15 <http://www.gov.cn/flfg/2010-04/30/content_1596420.htm> (accessed 26 March 2018).

Implementing Rules of the State Secrets Law¹⁶ and other regulations regarding the protection of state secrets in specific industries and sectors, such as mining, surveying and mapping, statistics and military sectors (collectively referred to as “State Secret Laws”).

7 State secrets are very broadly defined under the State Secret Laws. In general, any non-public information or matter that has a vital bearing on state security and national interests may be classified as a state secret and be subject to confidentiality measures. Information relating to national security, military and foreign affairs, national economy, science and technology development and other strategic matters of the state constitutes a state secret if its disclosure may be deemed to harm national security and interests in the areas of politics, economy, national defence or foreign relations. The scope of state secrets is to be determined by the State Secrets Bureau in conjunction with other relevant government departments responsible for the protection of state secrets within their respective jurisdictions and may be adjusted by such government agencies from time to time. However, this may be complicated when the State Secrets Bureau can retroactively denote information as a state secret, and has previously done this, including material that has been released into the public realm.¹⁷

16 <http://www.gov.cn/zwggk/2014-02/03/content_2579949.htm> (accessed 26 March 2018).

17 In *Xue Feng's Case*, a China born US geologist was charged for purchasing data regarding Chinese oil wells under a commercial contract at a time when such information had not yet been classified as secret, and was sentenced to eight years imprisonment for the crime of “gathering intelligence” and “unlawfully sending abroad state secrets”. The information involved was the co-ordinates of more than 30,000 oil and gas wells belonging to China National Petroleum Corp. For reports and comments about the case, see Forbes, “The Uncurious Case of Xue Feng’s Jail Sentence” <<https://www.forbes.com/2010/07/07/xue-feng-stern-hu-state-secrets-opinions-contributors-john-lee.html#36c1259f4dd4>> (accessed 26 March 2018); BBC, “China Jails US Geologist for Stealing State Secrets” <<http://www.bbc.com/news/10505350>> (accessed 26 March 2018) and Jerome A Cohen, “How China Handles ‘State Secret’ Prosecutions: Xue Feng’s Case” (South China Morning Post), the English version of the article is available at <<https://usali.org/publications/how-china-handles-state-secret-prosecutions-xue-fengs-case>> (accessed 26 March 2018). See also “State Secrets in China: What You Need to Know”

(continued on the next page)

8 Without approval by competent departments, no document or other material or objects classified as a state secret or information containing state secrets may be carried, transmitted, posted or transferred out of China. In practice, restrictions for cross-border transfer of state secrets may be triggered by multinational enterprises or Chinese enterprises with overseas operations when facing document production requests by overseas regulators and litigation discovery process.¹⁸

b Personal financial information and credit information

9 Several financial regulations promulgated in recent years contain data localisation requirements for personal financial information and credit information. For example, the Notice of the People's Bank of China on Urging Banking Financial Institutions to Strengthen the Protection of Personal Financial Information ("2011 PBOC Notice")¹⁹ issued by the People's Bank of China ("PBOC") in 2011 requires banks²⁰ to process personal financial information collected in China locally and not to transfer such information overseas.²¹ The Implementation

<<http://www.driven-inc.com/state-secrets-in-china-what-you-need-to-know/>> (accessed 26 March 2018).

18 For example, foreign banks that wish to expand in the US must make available to the Board of Governors of the Federal Reserve System all information on bank operations that the Federal Reserve deems necessary to enforce compliance with the applicable US laws. US regulators may request information about a Chinese bank or one of its customers that could be considered a state secret and the bank may find itself in a dilemma. Mitchell A Silk & Jillian S Ashley, "Understanding China's State Secrets Laws" <<http://www.chinabusinessreview.com/understanding-chinas-state-secrets-laws/>> (accessed 26 March 2018).

19 <http://www.gov.cn/gongbao/content/2011/content_1918924.htm> (accessed 26 March 2018).

20 In practice, it is controversial and not entirely clear whether the said notice (including data localisation requirements) also applies to non-banking financial institutions such as auto-finance companies, financial asset management companies, trust investment companies, financial companies and financial lease companies. According to this reporter's practical experience, some foreign auto-finance companies have considered that such data localisation requirements apply to them on an analogical basis.

21 According to the Notice of the People's Bank of China on Urging Banking Financial Institutions to Strengthen the Protection of Personal Financial Information, "personal financial information" refers to personal information

(continued on the next page)

Measures of the People's Bank of China for Protecting Financial Consumers' Rights and Interests²² issued by PBOC in 2016 provides exceptions to this rule for transferring such information abroad, including situations where (a) the transfer has been authorised by the data subject; (b) the information is transferred to the bank's overseas affiliates such as the head office, parent company or branch companies, subsidiaries or other affiliated institutions required for completing the business; and (c) the transferring party shall require the receiving party to effectively protect information through contracts and conducting on-site inspection.

acquired, processed or stored by a banking financial institution in its business operations or through the Credit Reporting System, the Payment System or any other system of the People's Bank of China, including:

- (a) personal identity information, including name, gender, nationality, ethnic group, type and valid term of identity certificate, occupation, contact information, marital status, family status, address of domicile or employer, and photo;
- (b) personal property information, including income, immovable property, vehicle, amount of tax, and amount paid for the provident fund;
- (c) personal account information, including account number, the time when an account is opened, bank at which an account is opened, account balance, and transactions made through the accounts;
- (d) personal credit information, including payments made to his credit card accounts, repayment of his loans, and other information formed in the process of personal economic activities and which can reflect his credit status;
- (e) personal financial transaction information, including personal information acquired, saved and retained by banking financial institutions in the course of operating the payments, settlement, financial management, safe deposit box or any other intermediary business and personal information generated in the course when clients have business relationships with insurance companies, securities companies, fund companies, futures companies and other third-party institutions through banking financial institutions;
- (f) derivative information, including consumption preferences, investment intent and other specific personal information formed by processing or analysing the source data; and
- (g) other personal information acquired or saved in the process of developing business relationships with individuals.

22 <<http://www.pbc.gov.cn/jingrxqy/145720/145728/3338677/index.html>> (accessed 26 March 2018).

10 The Regulation on Administration of Credit Investigation Industries (2015)²³ and the Decision of the State Council on Implementing Access Administration of Bank Card Clearing Institutions (2015)²⁴ also contain data localisation requirements. According to the regulations, credit reporting agencies are to store and process information collected within China. Bank card clearing institutions are required to deploy infrastructure capable of completing bank card clearing business independently and remote disaster system within China, and use such domestic infrastructure to process domestic bank card clearing business. Although the authorities do not clearly articulate the rationale for such localisation requirements, commentators consider that such regulations are mainly driven by the demand for protecting national financial security.²⁵

c Human genetic resources

11 Research and development (“R&D”) activities involving human genetic resources by the pharmaceutical industry may invoke regulations on cross-border transfer of Chinese human genetic resources. The collection, storage, R&D and export of Chinese human genetic resources has been subject to strict regulation since the promulgation of the Interim Measures for the Administration of Human Genetic Resources (1998) (“HGR Interim Measures”)²⁶ by the Ministry of Sciences and Technology (“MOST”) in 1998. According to the HGR Interim

23 <http://www.gov.cn/zwgg/2013-01/29/content_2322231.htm> (accessed 26 March 2018).

24 <http://www.cbrc.gov.cn/chinese/home/docDOC_ReadView/65DE69495F56495391C2FD56EEFE05DA.html> (accessed 26 March 2018).

25 For example, Art 5 of the Decision of the State Council on Implementing Access Administration of Bank Card Clearing Institutions (2015) provides that for protecting financial information security, when using a bank card issued within China in China, the relevant transaction shall be handled by the domestic bank card clearing infrastructure. See China Law Insight, “The Bank Card Clearing Rules Welcomes Post-UnionPay Age” <<https://www.chinalawinsight.com/2015/04/articles/corporate/mergers-acquisitions/new-bank-card-clearing-rules-heralds-a-post-unionpay-era/>> (accessed 30 April 2018).

26 <http://www.most.gov.cn/bszn/new/rlyc/wjxz/200512/t20051226_55327.htm> (accessed 26 March 2018).

Measures, any export of human genetic resources from China is to be approved by MOST.

12 In February 2016, the State Council released a draft regulation²⁷ on the administration of human genetic resources for public comments, which, once adopted, would replace the HGR Interim Measures. Human genetic resources are defined as “resources and materials, such as human organs, tissues, cells, nucleic acid and nucleic acid products which contain human genome, genes or gene products, *as well as any information derived from such resources and materials*”, amended to include information derived from physical human genetic materials. Under the draft regulation, foreign entities must collaborate with legal persons established in China in order to collect, store, export and conduct R&D of Chinese human genetic resources. Any Sino-foreign collaboration projects will remain subject to prior approvals. As a sign of the Government’s increasing awareness of cross-border electronic data transmission in R&D activities involving Chinese human genetic resources, the draft specifically emphasises that any form of cross-border movement of Chinese human genetic resources cannot be done without prior approval from the Government.²⁸ The draft regulation also requires Chinese and foreign parties to obtain informed consent of the data subjects in writing for the transfer of their human genetic resources.

27 Regulation on Human Genetic Resources (Ministry of Sciences and Technology Submitted Version), <<http://zqyj.chinalaw.gov.cn/readmore?listtype=1&id=970&1494395714812>> (accessed 26 March 2018).

28 Sidley Austin LLP, “China Issues New Regulation on Human Genetic Resources” <<https://www.lexology.com/library/detail.aspx?g=61c50844-2458-46ed-82ad-5846f8a247c6>> (accessed 26 March 2018). According to the draft regulation, the Ministry of Sciences and Technology (“MOST”) may reject an export application if: (a) the collaborator lacks the relevant capacity; (b) the purpose of collaboration is unclear, illegal or the term of the collaboration is unreasonable; (c) the plan of international collaboration and export is unreasonable; (d) the source of human genetic sources is illegal; (e) the application fails to pass the ethics commission of the collaborating parties; (f) the intellectual property ownership or distribution plan is unreasonable; (g) the export may endanger national security, national interest and public security; or (h) if there are other circumstances prohibited by laws and regulations. MOST periodically publishes the collaboration projects it has approved (<<http://www.most.gov.cn/bszn/new/rlyc/jgcx/index.htm>> (accessed 26 March 2018)).

d Demographic health information

13 The Interim Measures for the Administration of Demographic Health Information (2014) (“DHI Interim Measures”)²⁹ issued by the National Health and Family Planning Commission prohibits medical institutions from storing demographic health information in any server outside China as well as the hosting or leasing of any server outside China for the processing of demographic health information. The DHI Interim Measures seeks to strengthen the administration, security and privacy of the collection, use and management of demographic health data by all levels and all types of medical, health and family planning agencies, including licensed medical institutions. “Demographic health information” includes both individual personal health data as well as aggregated population health data. However, it remains unclear whether the DHI Interim Measures also applies to other entities obtaining demographic health information from medical institutions.

e Location and mapping data

14 The rapid development of smart devices and location-based online services gives rise to the demand for cross-border transfer of location and mapping data. The cross-border transfer of location and mapping data may invoke regulations in two overlapping areas. Firstly, some location and mapping data may constitute state secrets in surveying and mapping areas and will thus be subject to the regulations safeguarding state secrets. For instance, co-ordinates with a particular level of precision or co-ordinates of certain key facilities are classified as state secrets under the Measures on the Scope of State Secrets in the Administration of Survey and Mapping (2002)³⁰ and its attachment Catalogue of State Secrets in the Administration of Survey and Mapping, and are therefore prohibited from being stored and transferred out of China. Secondly, the regulations on map services, *ie*, the Regulations on Map Administration (2015),³¹

29 <<http://www.nhfpc.gov.cn/guihuaxxs/s10741/201405/783ec8adebc6422bbebdf79db3868d0b.shtml>> (accessed 26 March 2018).

30 <www.sbsm.gov.cn/accessory/200804/1207805182395.doc> (accessed 26 March 2018).

31 <http://www.gov.cn/zhengce/content/2015-12/14/content_10403.htm> (accessed 26 March 2018).

imposes data localisation requirements on map data even if the data do not constitute state secrets. Pursuant to these regulations, Internet map service providers are required to store map data in servers in China and implement the corresponding data security protection systems.

f Other regulations

15 Some other Internet regulations, such as the Provisions on the Administration of Online Publishing Services (2015),³² the Interim Measures for the Administration of Online Taxi Booking Business Operations and Services (2016),³³ and the Draft of Notice on Regulating Business Operation in Cloud Service Market (2016),³⁴ require the servers and data storage of these service providers to be hosted within China.

ii Practical implications of these regulations

16 In general, the effects of regulations promulgated before the Cybersecurity Law is limited in practice, and most cross-border data transfers from China were largely unregulated. This may be due to the light punishment under the regulations, rare implementation activities, and the absence of a centralised regulatory authority on cross-border data transfers.

17 Besides the state secrets laws and regulations which provide severe punishment that include criminal liability for violation, the punishment for violating the cross-border data transfer provisions under most other regulations is usually light. For example, financial institutions and medical institutions that violate the relevant personal financial information regulation or regulation on demographic health may be warned, be ordered to rectify or be criticised in a circulated notice. Chinese human genetic resource transferred from China without MOST

32 <<http://www.miit.gov.cn/n1146290/n4388791/c4638978/content.html>> (accessed 26 March 2018).

33 <<http://www.miit.gov.cn/n1146295/n1146557/n1146624/c5218603/content.html>> (accessed 26 March 2018).

34 <<http://www.miit.gov.cn/n1146295/n1652858/n1653100/n3767755/c5381367/content.html>> (accessed 26 March 2018).

approval may be confiscated. These regulations do not provide severe punishments such as monetary fines, revoking licences or the suspension of business.

18 Furthermore, before the Cybersecurity Law, restrictions for cross-border transfers of data were scattered in industrial or sectoral specific regulations and implemented by the relevant industrial regulators with no centralised co-ordinating authority. The absence of a centralised authority leaves regulatory loopholes in practice, since industrial regulators only have jurisdiction over cross-border data transfers by entities in their industries and cannot effectively extend their jurisdiction to other ordinary enterprises transferring the same data. For example, pharmaceutical companies, smart device providers and online medical platforms may also collect, obtain and transfer demographic health information abroad. However, they are not medical institutions and do not fall into the jurisdiction of the National Health and Family Planning Commission, the implementing authority of the DHI Interim Measures. This renders the cross-border transfer of personal health information of these companies largely unregulated in practice.

19 In addition, the enforcement of these regulations is generally weak in practice. Few implementation activities have been taken by the authorities in public reporting, and besides the area of state secrets, few cases can be located in publicly available sources.³⁵

35 There is some enforcement action in the area of state secrets (see para 8, n 18 above). In particular, in *Rio Tinto's Case*, four staff members of Rio Tinto were charged for stealing state secrets of China, including some detailed operation data regarding the stock of raw materials, production arrangement and sales information of a dozen Chinese iron and steel companies. The charge was later amended to that of stealing commercial secrets. Some reports and comments about *Rio Tinto's Case*, in particular, the state secrets issue in the case, are available at <<http://finance.sina.com.cn/chanjing/gsnews/20090715/18456484814.shtml>; <https://blogs.wsj.com/chinarealtime/2009/07/09/murky-state-secrets-laws-at-issue-in-rio-tinto-case/>>; <<http://www.nytimes.com/2010/03/30/world/asia/30riotinto.html>> and <<http://www.sandiegouniontribune.com/sdut-china-rio-tinto-employees-detained-070909-2009jul09-story.html>> (accessed 26 March 2018).

C CYBERSECURITY LAW AND ANCILLARY REGULATIONS

i *Data localisation requirements under Cybersecurity Law*

20 As introduced above, one significant legislative development of the Cybersecurity Law is that it explicitly provides data localisation requirements at the level of national laws in China for the first time. The data localisation requirements under the Cybersecurity Law apply only to critical information infrastructure operators (“CIIOs”), who are required to store the personal information and important data collected and generated in the course of their operations within China and may only transfer such information and data abroad due to business needs and upon security assessments by the relevant authorities (Article 37). The following key concepts are crucial to understanding these data localisation requirements:

- (a) *Network operators and CIIOs.* The Cybersecurity Law primarily imposes data security requirements on two key types of organisations – network operators and CIIOs. “Network” is broadly defined as “networks and systems that are composed of computers and other information terminals and the relevant facilities and are used for the purpose of collecting, storing, transmitting, exchanging and processing information in accordance with certain rules and procedures”, while “network operators” are defined as “owners and administrators of networks and network service providers” (Article 76). Such sweeping definitions not only cover providers of telecommunication or Internet services but may also encompass any public or private entities that own or operate IT networks for internal usage.³⁶

36 In past regulations, a more frequently used term is “network service provider”, which includes both Internet service providers (“ISPs”) and Internet content providers (“ICPs”). However, the network provided under the Cybersecurity Law also includes LAN and the industrial control system, which may not provide commercial or public services to society but shall also implement the relevant cybersecurity protection obligations. Therefore, “network operator” is defined very broadly to include the owner and administrator network and network service provider. See Yang Heqing, *The Paraphrase of the Cybersecurity Law of the People’s Republic of China* (China Democracy and Law Press, 2017) at p 153.

CIIOs are a subset of network operators subject to heightened cybersecurity requirements under the Cybersecurity Law. The Cybersecurity Law vaguely defines critical information infrastructures (“CII”) as information infrastructures in “public communication and information services, energy, traffic and transportation, irrigation, finance, public service, e-government and other key industries and sectors”, as well as other information infrastructures, “the damage, malfunction and data leakage of which may seriously endanger national security, national welfare, people’s livelihood, and public interest” (Article 31).³⁷ The Cybersecurity Law authorises the State Council to formulate regulations on the scope and protection requirements for CII. A draft regulation on the protection of CII was released in July 2017, further specifying the definition of CII and expanding its scope.³⁸ Telecommunication networks, broadcast and television networks, Internet and other information networks, and entities providing cloud computing, big data services and other types of large scale public information networks, which are not clearly mentioned in the definition of CII under the Cybersecurity Law, are included in the scope of CII under the draft regulation.

- (b) *Personal information.* The Cybersecurity Law provides a unified definition for “personal information” under Chinese law

37 The definition of critical information infrastructures (hereinafter “CII”) has changed with each of the law’s three drafts. In the first draft, “CII” was defined as a similar group of public utilities along with networks with a large number of users. In the second draft, the specific scope of “CII” was left to be determined by the State Council.

38 The Cyberspace Administration of China released the Draft Regulation on Security Protection of Critical Information Infrastructure on 10 July 2017 for public comments until 10 August 2017. The regulation is based on Art 31 of the Cybersecurity Law which authorises the State Council to formulate measures on the specific scope and protection requirements of CII. According to the Notice of General Office of the State Council on the 2016 Annual Legislative Plan of the State Council, the State Council entrusts the Cyberspace Administration of China (hereinafter “CAC”) to draft the regulation on CII protection. Since the regulation should be adopted in the form of an administrative regulation of the State Council, the draft regulation would be submitted to and adopted by the State Council at a later stage.

(Article 76) for the first time. The Cybersecurity Law follows the predominant way of using identification criteria to define personal information adopted by most jurisdictions and defines personal information as “all kinds of information recorded in electronic or other forms, which can be used, independently or in combination with other information, to identify a natural person’s personal identity”, which “includes but is not limited to the natural person’s name, date of birth, identity certificate number, biology-identified personal information, address and telephone number”.

- (c) *Important data.* “Important data” was first introduced into law by the Cybersecurity Law but was left undefined (Article 31). The Cybersecurity Administration of China (“CAC”), the most important co-ordinating and implementing authority of the Cybersecurity Law, has formulated draft guidelines which enumerates important data across industries, as further introduced below.

21 In general, the aforesaid data localisation provision under the Cybersecurity Law remains high level and fails to be specific in relation to important matters such as the scope of important data and the criteria and procedures for security assessment on the export of personal information and important data outside of China by CIIOs. Such ambiguity leaves plenty of room for the discretion of the regulatory authorities in formulating implementing rules.

22 Companies face increased penalties for non-compliance with the Cybersecurity Law. CIIOs violating the aforesaid data localisation requirements could trigger a wide range of potential penalties including warnings, suspensions of operation, the revoking of business licences and permits, and fines up to RMB500,000 (Article 66).

ii Draft Data Export Measures

23 Following the promulgation of the Cybersecurity Law, CAC, the major implementing authority of the Cybersecurity Law, formulated a series of ancillary regulations and draft regulations of the Cybersecurity Law. *Inter alia*, CAC released the Measures for Security Assessment of

the Cross-Border Transfer of Personal Information and Important Data on 11 April 2017 for public comments.³⁹ Later, on 19 May 2017, CAC released a revised draft of the Measures for Security Assessment of the Cross-Border Transfer of Personal Information and Important Data in a close-door seminar with various enterprise representatives (collectively referred to as “Draft Data Export Measures”).⁴⁰ The Draft Data Export Measures sets out the basic framework for security assessment of data exports, while more specific requirements are set out in the Draft Data Export Guidelines as introduced below. The Draft Data Export Measures operates a very significant deviation from the Cybersecurity Law by extending the requirements for data localisation and security assessments from “CIIOs” to all “network operators”.⁴¹

24 The key provisions of the Draft Data Export Measures are as follows:

- (a) *Personal information and important data collected and generated by network operators in the course of their operations within China in principle shall be stored in China.* The Draft Data Export Measures adopts a definition of “personal information” which is similar to the definition in the Cybersecurity Law, as introduced

39 <http://www.cac.gov.cn/2017-04/11/c_1120785691.htm> (accessed 26 March 2018).

40 CAC invited foreign company representatives and various other stakeholders to discuss and comment on the revised draft measures at the seminar. Issues discussed during the seminar included the deviation of the draft measures from the Cybersecurity Law, with network operators indicating that they would rather CIIOs were subject to security assessment, and that data export measures would hamper international trade and foreign investment in China. See Grace Chen, “What We Don’t Know about China’s New Cybersecurity Law” <<https://www.law360.com/articles/931757/what-we-don-t-know-about-china-s-new-cybersecurity-law>> (accessed 26 March 2018).

41 CAC did not publish the full text of the revised draft. A leaked version is online and is available in “China Releases Near-final Draft of Regulation on Cross-Border Data Transfer” <https://www.cov.com/-/media/files/corporate/publications/2017/05/china_releases_near_final_draft_of_regulation_on_cross_border_data_transfers.pdf> (accessed 26 March 2018). Since the draft only governs the export of data outside of China, this reporter uses “Draft Data Export Measures” rather than “Draft Cross Border Data Transfer Measures” as the abbreviated name for the measures.

above.⁴² The Draft Data Export Measures vaguely defines important data as “data closely related to national security, economic development and public interests” for the first time and leaves its specific scope to be determined by the relevant national standards, with important data identification guidelines to be formulated in the future.

- (b) *Express “notice – consent” requirements for exports of personal information.* The Draft Data Export Measures, for the first time, clearly requires network operators to inform concerned individuals as to the purpose, scope, content and the receiving country or region of the data export and obtain their consent to the export. Personal information cannot be exported if individuals’ consent is not obtained, and whether individuals consent to the export of their personal information is part of the assessment process. Consent for data exports is not required either (i) in circumstances where the security of citizens’ lives and properties is endangered, or (ii) where individuals’ consent can be deemed obtained, in cases of international calls, international e-mails, international instant messaging, cross-border e-commerce, or through other active behaviour.
- (c) *Self-assessment is required for exports which do not trigger criteria for submission to the Government.* All network operators are required to carry out self-assessments for export of data before export and shall be responsible for the assessment results.
- (d) *Focus of assessment.* The assessment of data exports is to be focused on the following aspects:
 - (i) lawfulness, appropriateness, and necessity of the data export;
 - (ii) the volume, scope, type, sensitivity of personal information and whether the data subjects consent to the export of their personal information;
 - (iii) the volume, scope and type of important data;
 - (iv) the security protection capability, measures and environment of the transferring party and receiving party;
 - (v) risk of the data being divulged, damaged, tampered with or misused; and

42 See para 20(b) above.

- (vi) risks for national security, public interest and the individual's legitimate interests.
- (e) *Submission to government assessment is required if certain criteria is met.* In the event that exports of data meet the following criteria, network operators must submit their case to their industrial regulatory authorities or CAC⁴³ for assessment:
 - (i) the data containing personal information of more than 500,000 people;⁴⁴
 - (ii) the data relating to nuclear facilities, chemistry and biology, national defence and military, population health, and data of mega projects, ocean environment, sensitive geographical information, *etc*;
 - (iii) the data including cybersecurity information in relation to system loopholes, security protection and others of CII;
 - (iv) CIIOs transfer personal information and important data to overseas parties; or
 - (v) there are other situations which may affect national security and societal public interests, and the industrial administration authority or regulatory authority considers the export data should be subject to the security assessment.
- (f) *Circumstances where data exports are prohibited.* Data are prohibited from export if:
 - (i) the concerned individual has not consented to the export or his/her interests may be jeopardised;
 - (ii) national security or public interests may be endangered, or
 - (iii) there exist other circumstances prohibited by the competent authorities in their discretion.
- (g) *Ongoing assessment and report obligation is also provided.* Network operators shall conduct security assessments of data exports at

43 In principle, network operators are to submit to their corresponding industrial regulatory authorities for assessment (for example, financial, telecommunication, irrigation and equipment manufacturing authorities). For network operators which do not have a specific industrial regulatory authority, they shall submit to CAC for assessment.

44 As *per* the Cybersecurity Law, the Draft Data Export Measures does not distinguish whether such personal information belongs to Chinese citizens. As a result, any personal information collected or generated within China, regardless of the nationality of the data subject, may fall within the scope of this provision.

least once a year and promptly report the results to the relevant industrial or regulatory authority. Where significant changes in purpose, scope, volume, type and other aspects occur to the data export or the recipient or exported data have a significant security incident, prompt re-assessments are required to be carried out.

iii *Personal Information Security Specification*

25 The Cybersecurity Law emphasises the role of standards in implementing its provisions.⁴⁵ With the promulgation of the Cybersecurity Law, the National Information Security Standardization Technical Committee (“TC 260”) has been stipulating and revising a series of national standards concerning cybersecurity.⁴⁶ Among other things, TC 260 promulgated the Personal Information Security Specification (GB/T 3527-2017) (“PIS Specification”).⁴⁷ The PIS Specification creates a comprehensive framework and imposes strict protection requirements throughout the data life cycle. It is the most important national standard in the implementation of data privacy protection requirements under the Cybersecurity Law. Although the PIS

45 For example, Art 15 of the Cybersecurity Law provides that:

[T]he state shall establish and improve the system of cybersecurity standards. The standardization administrative department of the State Council and other relevant departments of the State Council shall, according to their respective functions, organize the formulation of and revise at appropriate time national and industry standards relating to cybersecurity administration and the security of network products, services and operations.

46 According to the *Several Opinions on Strengthening National Cybersecurity Standardization Work* published by CAC (2017), the promulgation of standards in CII protection, cybersecurity review, trustworthy identity in cyberspace, key information technology products, cyberspace confidentiality protection and supervision, big data security, personal information protection, smart city security, security of the Internet of things, new generation communication network security Internet TV terminals security, Internet security information sharing and others are the focus and priority. The drafts of these standards are published on the official website of TC 260 for public comments, <<http://www.tc260.org.cn/front/bzzqyjList.html?start=0&length=10>> (accessed 26 March 2018).

47 <<http://c.gb688.cn/bzgk/gb/showGb?type=online&hcno=4FFAA51D63BA21B9EE40C51DD3CC40BE>> (accessed 26 March 2018).

Specification is a voluntary standard, it is likely to serve as a referential basis for the enforcement by regulatory authorities, as its draft has already been used by regulatory authorities in the examination and audits of Internet companies even before its formal adoption. The PIS Specification contains the following major provisions relating to cross-border data transfer issues:

- (a) *Personal information.* The PIS Specification uses two criteria to define personal information, (i) information identifiable to a specific data subject, or (ii) information related to a specifically identified data subject. It provides a non-exhaustive list of personal information. Device identifiers such as MAC address, IMEI and IP address are included in the scope of personal information.
- (b) *Sensitive personal information.* The PIS Specification provides a broad definition of sensitive personal information, which is defined as any personal information that would endanger the personal or property safety, cause harm to the reputation or physical or mental health, or lead to discriminatory treatment of data subjects. Information commonly processed by financial institutions, such as phone numbers, account numbers, transaction records, credit records, deposit information and virtual currencies of data subjects are categorised as sensitive personal information. Collection of sensitive personal information shall be based on informed, explicit, specific and freely given consent of data subjects.
- (c) *Required content regarding cross-border transfer in privacy policies.* The PIS Specification sets out the content required to be included into the privacy policies of service providers, and provides some standard clauses for privacy policies. Among other things, privacy policies shall set out whether and for what purpose users' personal information would be transferred abroad, the type of personal information to be transferred, the contractual or legal basis for cross-border data transfer, and the security protection measures for cross-border data transfer (eg, whether the personal information would be anonymised for the transfer). Apart from the aforesaid requirements for privacy policies, the PIS Specification does not include other specific requirements for cross-border data transfer, and leaves such

requirements to the forthcoming data export guidelines (as introduced below).

iv *Draft Data Export Guidelines*

26 TC 260 has been stipulating the draft of the Information Security Technology Guidelines for Cross-Border Data Transfer Security Assessment and released a first draft of it on 27 May 2017 and a revised version on 30 August 2017 (collectively referred to as “Draft Data Export Guidelines”). The Draft Data Export Guidelines offers detailed guidance for security assessment on data exports. The Draft Data Export Guidelines indicates it is also a non-compulsory guideline.⁴⁸ However, it is likely to be used by enterprises for assessment in practice, and also by regulators in enforcing the cross-border data transfer assessment measures. The key provisions of the Draft Data Export Guidelines are summarised as follows.

a Application

27 The Draft Data Export Guidelines applies to security assessments carried out by network operators. It also applies to the competent industry regulators or regulatory authorities in their guidance and supervision of the security assessments carried out by network operators. CAC and the competent industry regulators or regulatory authorities may refer to the Draft Data Export Guidelines in the security assessments of data exports carried out within their respective authorities.

b Clarification of the definition of data export

28 The Draft Data Export Guidelines clarifies that the following circumstances shall be deemed as “data export”:

- (a) personal information and important data are provided to any entity within China who is not subject to the jurisdiction of China or not registered in China;

48 The title of the guidelines is “GB/T”, the abbreviation of the Chinese phonetic alphabet of “national standard, recommended” (Guobiao/Tuijian).

- (b) data which are not transferred or stored outside China are accessed and viewed by overseas institutions, organisations and individuals (except for public information and webpage visits); and
- (c) a company group exports its internal data which involve personal information and important data collected and generated in the course of its operations within China.

29 The following circumstances shall not be deemed “data exports”:

- (a) export of personal information and important data in transit in China; and
- (b) outsourcing exemption, *ie*, export of personal information and important data not collected or generated in the course of operations in China but being processed in China for outsourcing purposes.

c Identification of important data

30 Personal information and important data are subject to rules on data security. The Draft Data Export Guidelines enumerates important data in 28 industries and sectors, such as the resources and energy, telecommunications and electronic manufacturing industries. The definition, scope and criteria for identifying important data in these key industries may be further specified by the competent industry regulators or regulatory authorities. The provisions regarding important data under the Draft Data Export Guidelines reflect some restrictions for data exports in existing laws and regulations (such as demographic health information, personal financial information, credit information and map information), and add new types of data restricted from being exported, such as registration information of e-commerce platforms and e-commerce transaction records.

d Clarification of the “notification – consent” requirement for the export of personal data.

31 The Draft Data Export Guidelines further specifies the requirement of “notification – consent” for the export of personal data in the assessment on lawfulness. Prior to obtaining consent from the

individuals whose personal information is to be exported, the network operators are to expressly notify such individuals of the purpose, type, recipient and risks of the data export as well as its contact person and contact details.

32 When the privacy policy of the network operator or the recipient of exported data changes, or when there is a major change in the purpose, scope, type, quantity or risks of the data export, consent is to be re-obtained from the individuals whose personal information is to be exported.

33 Moreover, the Draft Data Export Guidelines expressly provides that export of *personal information which has been lawfully disclosed to the public* shall be deemed an export with the consent of the data subject.

e Clarification of circumstances triggering security self-assessments

34 The Draft Data Export Guidelines requires network operators to carry out security self-assessments every year. Self-assessment shall be initiated in the following circumstances:

- (a) the business of network operators involves data exports;
- (b) before CIIOs export data;
- (c) after the data is exported upon self-assessment, when there is a major change in the purpose, scope, type, quantity and other aspects of the data export, the recipient changes, or the recipient has a major security incident; and
- (d) as required by the competent industrial regulatory authorities or CAC in their discretion.

35 The Draft Data Export Guidelines makes the following clarification regarding the threshold of self-assessment:

- (a) “Continuous export” shall only be subject to one assessment, and the “continuous export” refers to “data exports that have the same purpose and recipient with no significant change in the scope, type and quantity and the interval between two exports being less than one year”.

- (b) In the case of multiple parties involved in a data export (*eg*, when using cloud services or subcontracting services), the originator of the data export shall be responsible for the security self-assessment.⁴⁹

f Security assessment process

36 Business units of network operators who need to export data shall prepare data security plans, which shall include:

- (a) the type, volume, scope and sensitiveness of personal information;
- (b) the type, volume and scope of important data;
- (c) the information systems involved in the transfer;
- (d) the security protection capability of the exporting party; and
- (e) the security protection capacity of the receiving party and the overall security environment of the receiving country.

37 Network operators are required to establish data export security self-assessment working groups, which shall mainly consist of professionals in law, policy, security, technology, management and other areas. The work group shall review data export plans submitted by the business units and regularly carry out inspections and spot checks on the data exports.

38 Where the approval of CAC and the industry regulatory authorities is required for the data export, the network operator shall submit the assessment report to CAC and the industry regulatory authority for approval prior to such export. Like the Draft Data Export Measures, the Draft Data Export Guidelines also requires network operators to submit security self-assessment reports to the industry regulatory authority or

49 For example, if a cloud service client actively requests a cloud service provider to make a data export, the cloud service provider shall co-operate with the cloud service client to carry out the security self-assessment and the cloud service client shall assume the corresponding responsibilities. If the cloud service provider actively proposes to make a data export, the cloud service client shall co-operate with the cloud service provider to carry out the security self-assessment and the cloud service provider shall assume the corresponding responsibilities.

CAC (if there is no definitive industry regulatory authority) under the circumstances similar to those specified in the Draft Data Export Measures (as introduced above).⁵⁰

g Focus of assessment

39 The self-assessment for data export mainly focuses on two issues: (a) the purpose of the data export, including the lawfulness, appropriateness and necessity of the export; and (b) the risk controllability of the export.

- (a) The purpose of the data export shall be lawful, appropriate and necessary, which shall be assessed on the basis of the following dimensions: (i) whether the export is prohibited by the laws and regulations, or by the relevant authorities; (ii) for personal information, whether the consent of the data subject has been obtained; (iii) whether the data export complies with provisions under relevant international treaties; (iv) whether the data export is necessary for performing the ordinary business activities or the contractual obligations of the network operators; (v) whether the data export is required for judicial assistance; and (vi) whether the data export is necessary for protecting the cyber sovereignty, national security, public interest and lawful interest of citizens.
- (b) The risk controllability assessment shall take into account (i) the levels of impact of the data export and (ii) the possibility of security incidents during the data export.

The level of impact of data export means, for personal information, the level of impact on personal rights and interests caused by the export of the personal information, and for important data, the impact on national security and social public interests caused by the export of the important data. The level of impact shall be assessed on the basis of the volume, scope, type, sensitivity of the personal information or important data and how such data are processed (which means whether such data are anonymised or desensitised).

50 See para 24(e) above.

The possibility of security incidents during the data export shall be assessed from the following factors: (i) technical and management capability of the exporter;⁵¹ (ii) technical and management capability of the recipient;⁵² and (iii) the political and legal environment of the jurisdiction of the recipient.⁵³

h Assessment methods

40 If the first step of assessment (purpose assessment) finds that the purpose of data export is not lawful, appropriate or necessary, the data shall not be exported.

41 If the data export is lawful, appropriate and necessary, then the risk controllability shall be assessed, including the level of impact and the possibility of a security incident, as introduced above. The Draft Data Export Guidelines identifies factors and criteria for rating the level of impact and the possibility of a security incident.⁵⁴ On the basis of a comprehensive judgment of the abovementioned factors, the overall security risk of data export activities is classified into four levels –

51 This includes whether the transferring party has established management systems, personnel management, contractual obligation, auditing mechanism, emergency response and complaint management systems to effectively prevent security incidents, and whether it has adopted advanced data security technologies.

52 This includes the background and qualifications of the receiving party, whether the transferring party has established management systems, personnel management, contractual obligation, auditing mechanism, emergency response and complaint management systems to effectively prevent security incidents, and whether it has adopted advanced data security technologies.

53 This includes whether the receiving jurisdiction has any laws, regulations and standards on protecting personal information, whether it has joined any international or regional organisations relating to personal information protection, has signed any international and regional treaties regarding data flow, and the government authorities' power of and procedure for access of personal information in the jurisdiction.

54 For example, if the personal information exported is mainly sensitive personal information, the level of impact shall be increased a level. If the personal information exported is anonymised, the level of impact shall be lowered a level. If the transferring party has established sound management systems which can effectively prevent the occurrence of security incidents, its protection capability shall be deemed high and the level of possibility of a security incident shall be lowered.

extremely high, high, middle and low. If the security risk of the data export is extremely high or high, the relevant personal information or important data cannot be exported.

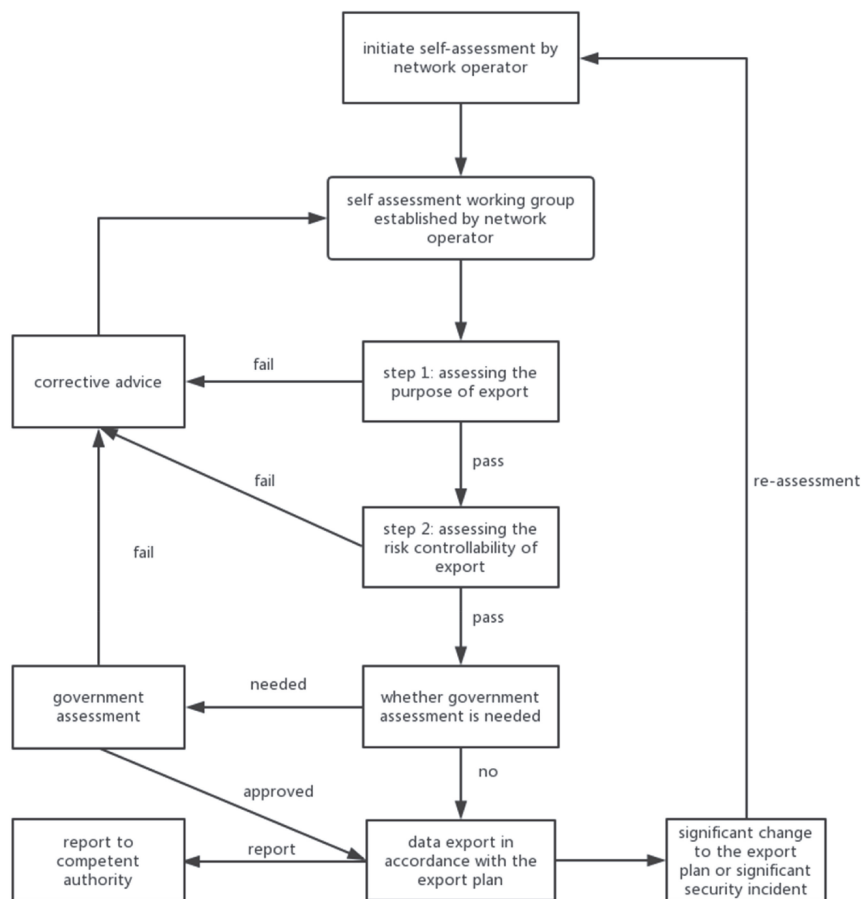


Chart 1 Self-Assessment Process⁵⁵

i Process and requirements for government assessment

42 A government security assessment shall be triggered in the following circumstances:

⁵⁵ Chart 2 of the Information Security Technology Guidelines for Cross-Border Data Transfer Security Assessment, “Self-Assessment Process of Data Export”.

- (a) when a network operator is required to submit its self-assessment report to the competent regulatory authority for review under the circumstances listed above;⁵⁶
- (b) when a large number of users complain about or report a violation by network operators;
- (c) when a national trade or trade association suggests a government assessment; or
- (d) when CAC or the industrial regulatory authority deems necessary to perform a government assessment at their discretion.

43 The assessment shall be carried out in the following steps:

- (a) The assessing authority (CAC or the industrial regulatory authority as the case may be) shall formulate an assessment plan, which shall specify the target and scope of the government assessment, establish an assessment working group, and determine the assessment procedures and methods.
- (b) The assessment working group shall follow the assessment plan, conduct assessment through remote monitoring and on-site inspection in accordance with the Draft Data Export Guidelines, and produce a report on the government security assessment. Such an assessment report shall specify the assessment results and the grounds thereof, the major risk exposures, and recommended corrective actions for the data exports.
- (c) CAC and the industry regulatory authority shall establish an expert committee, comprised of cyber security experts, data security experts and experts in the relevant fields or industries. The expert committee shall analyse and review the self-assessment reports submitted by the network operators or the assessment report produced by the assessment working group and issue an advice.
- (d) CAC or the industrial regulatory authority shall render a decision on whether the data can be exported on the basis of the assessment report and the advice of the export committee, and notify the network operators about its decision in writing.

56 See para 24(e) above.

- (e) CAC or the industrial regulatory authority may also carry out *ex post* inspections on the data export activities by the network operators periodically, based on the self-assessment or the government assessment results.

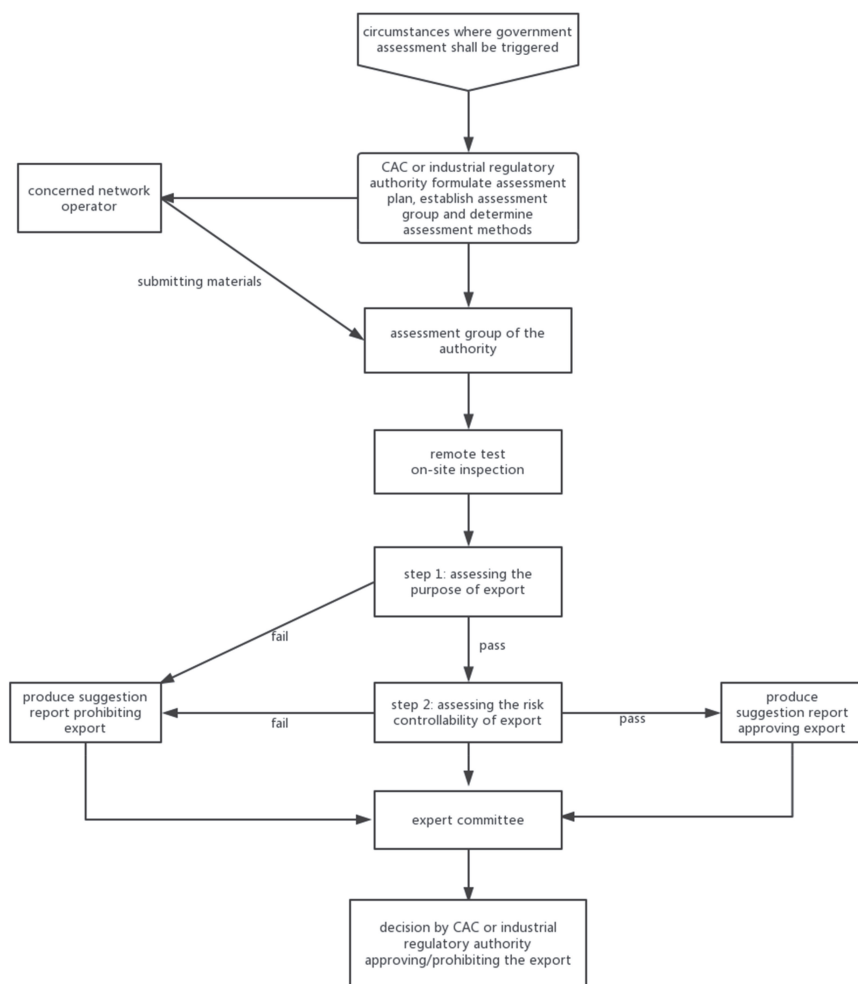


Chart 2 Government Assessment Process⁵⁷

⁵⁷ Chart 3 of the Information Security Technology-Guidelines for Cross-Border Data Transfer Security Assessment, "Government Assessment Process of Data Export".

D IMPLICATION AND PROSPECTS

44 The Cybersecurity Law created unprecedented restrictions on cross-border transfers of data from China. The Cybersecurity Law empowers CAC to steer the promulgation of the ancillary regulations and standards to co-ordinate the regulatory activities of the industrial regulators. The designation of CAC as the centralised regulatory authority may remedy the regulatory loopholes and enhance law enforcement.

45 Protection of the rights of the data subject is a theme of the cross-border data transfer rules under the Cybersecurity Law and the ancillary regulations, as the rules impose a “notice-consent requirement” for such personal information and require an assessment of the impact of such export. However, these rules are driven mainly by national security concerns. The Cybersecurity Law and the ancillary regulations introduce and define the concept of “important data”, which is aimed at protecting national and societal interests. According to Yanqing Hong, a drafter of the regulations, the cross-border data transfer rules address the threats of data security and national security in the era of big data – massive amounts of data are controlled by the private sector, the accuracy and value of which may even surpass government data, and hostile foreign forces may use such data to subvert the Chinese government, launch cyber-attacks and endanger Chinese national security.⁵⁸

46 Since the cross-border data transfer rules mainly aim to protect national security, they are far-reaching and leave regulatory authorities plenty of room for discretion. For instance, the threshold for triggering government assessment is low under the drafts and some factors required to be considered in the security assessment, such as the necessity of the

58 An example given is that of Alibaba, the Chinese e-commerce giant with more than 400 million users. The personal information and business data it controls can match the public security organ’s basic population database and even surpass it in accuracy. The leakage and damage of such data would create a serious threat to national security. See Yanqing Hong, “The Cross-Border Data Flows Security Assessment: An Important Part of Protecting China’s Basic Strategic Sources”, Working Paper, 20 June 2017, <<http://apide.org/apru-asia-eu-dialogue/readings/CrossBorderDataFlows.pdf>> (accessed 26 March 2018).

data export, the risk arising from the aggregation of the data after export, and the political and security environment of the receiving country, lack objective criteria. In addition, regulatory authorities retain the power to block a data export in circumstances where national security, economic development or social public interest may be endangered.

47 If the proposed measures and standards are adopted in the shape of the latest released drafts, almost all foreign and domestic enterprises with business operations in China would be subject to data localisation requirements and security assessment on data export.⁵⁹ The broad applicable scope of the draft measures and standards has been questioned by some Chinese enterprises and commentators as lacking sufficient legal basis in the Cybersecurity Law, and CAC has tried to justify it on the basis of the general requirements on ensuring that data are secure and controllable under the National Security Law.⁶⁰ It is not entirely clear whether the broad draft data export measures and standards reflect the political will of the higher levels of the Chinese government, or if they merely represent the position of CAC which may seek to assert its authority in this area.

48 Not surprisingly, the Cybersecurity Law and the ancillary regulations, in particular the data localisation requirements, have sparked outcry from the international community. Foreign companies worry that the data localisation requirements would make it even harder to do

59 Some enterprises (such as banks) may be subjected to both the existing regulations adopted before the Cybersecurity Law as well as the draft measures and standards. However, the draft measures and standards do not discuss how they would be reconciled with the existing regulations.

60 Article 25 of the National Security Law (2015) provides that:

[T]he state shall build a network and information security guarantee system, improve network and information security protection capability, strengthen the innovation research, development, and application of network and information technologies, realize the controllable security of the core technologies and crucial infrastructure of network and information and the information systems and data in important fields; strengthen network management, prevent, frustrate, and legally punish network attack, network invasion, network information theft, dissemination of illegal and harmful information, and other network-related infractions of law and crimes, and maintain the state's sovereignty, security, and development interests in the cyberspace.

business in China due to the increased costs to foreign firms, exposing multinationals to cyber-espionage, and giving domestic companies an unfair edge. The American Chamber of Commerce published a statement on the date of adoption of the Cybersecurity Law criticising the restrictions for cross-border data flows and security review under the law, claiming that it will “provide no security benefits but will create barriers to Chinese as well as foreign companies operating in industries where data needs to be shared internationally ... will unnecessarily weaken security and potentially expose personal information”.⁶¹

49 In May 2017, a coalition of business lobby groups comprising of 55 leading business associations and representing European, American and Asian companies called on the Chinese government to delay implementing the law, while the European Union Chamber of Commerce in China asked for additional time to allow companies to adhere because of the “substantial compliance obligations”.⁶² In the latest push back against the Cybersecurity Law, the US submitted a document to the World Trade Organization for debate, which stated that restriction for cross-border data transfer under the Cybersecurity Law and the draft ancillary regulations and standards “would disrupt, deter, and in many cases, prohibit cross-border transfers of information that are routine in the ordinary course of business” and “restrict even routine transfers of information, fundamental to any modern business”, and requested that China refrain from issuing or implementing final measures until the aforesaid concerns are addressed.⁶³

50 Facing huge international pressure, it remains to be seen whether the Chinese government will maintain its strong position on cross-border data transfers. As of today, the Draft Data Export Measures and Draft

61 <<https://www.amchamchina.org/about/press-center/amcham-statement/amcham-china-statement-on-cybersecurity-law>> (accessed 26 March 2018).

62 <<https://www.nytimes.com/2017/05/31/business/china-cybersecurity-law.html>>; <<http://www.reuters.com/article/us-china-cyber-law/foreign-business-groups-push-for-delay-in-controversial-china-cyber-law-idUSKBN188156>> (accessed 26 March 2018).

63 “Council for Trade and Services – Communication from the United States – Measures Adopted and under Development by China Relating to Its Cybersecurity Law” (Doc #: 18-1181, 23 February 2018, S/C/W/376).

Data Export Guidelines have not been formally adopted yet, and there are no formal enforcement actions relating to the data localisation requirements under the Cybersecurity Law on publicly available sources, but some multinational companies moved their data to China.⁶⁴ The struggle over cross-border data transfers between the Chinese government and the international business community may continue for a while.

⁶⁴ For example, Apple set up a data centre in Guiyang to store the data of Chinese iCloud users (<http://news.xinhuanet.com/2017-07/12/c_1121308086.htm> (accessed 26 March 2018)); and Airbnb moved the data of Chinese users in China (<<https://36kr.com/p/5055630.html>> (accessed 26 March 2018)).

Jurisdictional Report HONG KONG SAR (THE PEOPLE'S REPUBLIC OF CHINA)

Reporter: **Mark Parsons***
Partner, Hogan Lovells

A BACKGROUND INFORMATION

1 Hong Kong has a relatively unique position as a Special Administrative Region (“SAR”) of the People’s Republic of China (“PRC”). Under the “One Country, Two Systems” principle for the reunification of the PRC, Hong Kong retains a largely independent legal and regulatory system and a substantial degree of economic autonomy from the mainland.

2 Although Hong Kong’s role as the premier “gateway” for economic activity between the mainland PRC and the rest of the world is regularly said to be under challenge, from a practical business perspective, Hong Kong continues to be a vibrant hub of economic and financial activity in the PRC and for the wider Asia region. A substantial number of global multinational corporations have regional headquarters and operations in Hong Kong and commercial transactions in the region are regularly settled through Hong Kong financial institutions and under Hong Kong law contracts. Hong Kong has a substantial presence in areas such as securities trading, asset management, commercial banking and logistics, in large measure due to the strong reputation of its markets and regulators and the ready availability of expertise in these areas.

3 As elsewhere in the world, data flows are the lifeblood of business in Hong Kong. There are substantial data centre operations in Hong Kong, both captive operations controlled by businesses for their sole use

* The reporter gratefully acknowledges the contributions of Stephen Kai-yi Wong, the Privacy Commissioner for Personal Data of Hong Kong, China and his office to the responses to the questionnaire. All errors are this reporter’s own.

and serviced operations managed by vendors specialising in technology and data centre services. The adoption of cloud computing is on the rise in Hong Kong as elsewhere, and as of September 2017, Hong Kong's mobile telephone subscriber penetration rate stood at 247%. Hong Kong's economy is a "wired" economy, located at an international crossroads of activity.

4 It is in this context that the matter of cross-border data transfers must be viewed. Hong Kong has taken a relatively tentative approach to regulating international transfers of personal data. While Hong Kong's data protection law, in very general terms, regulates the collection and processing of personal data in much the same way as European data protection laws, the regulation of international transfers stands as an important exception. The restrictions on international transfer set out in the law have not been brought into effect in the 21 years that the law has been in force. When a comprehensive review of the law was undertaken commencing in 2009, some 43 reform proposals were put forward by the Constitutional and Mainland Affairs Bureau for public consultation. The consultation did not, however, include a proposal to introduce the international transfer restrictions.

5 The introduction of data transfer controls would raise important political considerations for Hong Kong, such as how data transfers to the mainland PRC, treated as a separate jurisdiction under "One Country, Two Systems" model, would be addressed and the scope Hong Kong would have to agree arrangements with other jurisdictions.

6 More fundamentally, there was significant opposition to the introduction of a data transfer control at the time that data protection was introduced to Hong Kong. Commentators queried the feasibility of businesses, particular smaller enterprises, implementing these requirements. Hong Kong's traditionally laissez-faire approach to business and economic regulation is an important aspect of these objections. Hong Kong imposes few controls on capital and currency flows across its borders, and it is a point of pride that it is relatively straightforward for foreigners to establish and get on with running a business in Hong Kong. To restrict international transfers of personal data would be perceived by some to be counter-productive to wider economic and trade agendas.

7 That said, it is also clear that from an economic and trade perspective, Hong Kong enjoys its position of receiving data from other jurisdictions in the region and strives to encourage multinationals to establish its regional hubs here. Tighter regulation of personal data could improve its competitive position as a hub jurisdiction, particularly now that recent years have seen a proliferation of data protection laws across the Asia-Pacific region, raising the competitive bar, and we now see those laws influenced by the advancing standards being set under the European General Data Protection Regulation.

8 There are of course fair arguments each way on these points, but at present the introduction of data export controls does not appear on the legislative agenda. Hong Kong's Legislative Council is currently evaluating the issue and has commissioned a study on the potential business impacts. As elsewhere, the development of data protection law in Hong Kong has in part been "event driven", the most salient example being the stepping up of direct marketing controls in Hong Kong in 2013 in the wake of a well-publicised enforcement action against Octopus Rewards. Events could also influence the policy direction for cross-border data transfers.

9 Looking at the issues more broadly, the fact that different jurisdictions across the Asia-Pacific region now have different rules for international transfers of personal data poses significant challenges for multinational businesses, whether based in Hong Kong or elsewhere in the region. The absence of unifying standards means that in practice, some jurisdictions have data localisation, some require opt-in consents, some enable other means of achieving compliant international transfers, such as reliance on "white lists" or the use of contract terms (the substance of which may also vary from jurisdiction to jurisdiction) and some have no restrictions at all. For many organisations these points of difference generate uncertainty and inefficiency, without it necessarily being the case that data subjects' interests are demonstrably advanced through, for example, improved data security or regulatory oversight. There are also concerns that governments' motivations for introducing international transfer restrictions are more a matter of trade policy and favouring domestic technology businesses than advancing individual rights in privacy or cybersecurity.

10 From this wider perspective, there is a clear and pressing need for interoperability of data protection regimes in the Asia-Pacific region. In the era of smart phones and cloud computing, it is very difficult to see how “hard” cross-border transfer restrictions (*ie*, localisation or consent-based systems) can realistically be complied with in practice. Accountability in fact is, in this reporter’s personal view, the worthier and more beneficial objective. One would expect to see greater progress towards better compliance outcomes in practice by advancing privacy by design, ensuring that organisations entrusted with personal data take adequate steps to process personal data in accordance with applicable standards and ensuring that there are effective means of enforcing these standards, as opposed to making assumptions based on geography alone.

B GENERAL LEGAL FRAMEWORK OF INTERNATIONAL DATA TRANSFERS

i *Existing data privacy protections in national legislation*

11 The Personal Data (Privacy) Ordinance¹ (“PDPO”) is comprehensive data protection legislation enacted in Hong Kong in 1995, with most of its principle provisions taking effect from 20 December 1996.² The PDPO is, to a material extent, modelled on the 1980 Organisation for Economic Co-operation and Development “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” (“OECD Model”).

12 The provisions of the PDPO apply to personal data of which the processing is controlled in or from Hong Kong. The PDPO regulates “data users”, defined as persons who either alone or jointly or in common with other persons, control the collection, holding, processing or use of personal data.

13 Section 33 of the PDPO imposes a restriction on international transfers of personal data, but this provision has not yet been brought

1 Cap 486.

2 <<https://www.elegislation.gov.hk/hk/cap486!en@2013-04-25T00:00:00/longTitle>> (accessed 20 March 2018).

into effect and a notice in the *Government Gazette* would be required in order for this to be the case.

14 The deferral of section 33 was due to concerns about the practicalities of implementing section 33 and potential adverse impacts on business, particularly small and medium-sized businesses. The absence of compliance guidance that would assist businesses in interpreting specific requirements of the cross-border transfer restriction was also cited as a concern.³

15 If it were brought into force as currently drafted, section 33 would apply to: (a) transfers of personal data from Hong Kong to a place outside Hong Kong; and (b) transfers of personal data between two other jurisdictions where the transfer is controlled by a Hong Kong data user.

16 Section 33's restriction on international transfers of personal data is framed under the PDPO as a general prohibition subject to a list of exceptions, as follows:

- (a) transfers to a place designated by the Privacy Commissioner for Personal Data ("PCPD") by notice in the *Gazette* as having been determined to have a law substantially similar to or serving the same purpose as the PDPO ("White List Jurisdiction");
- (b) the data user has reasonable grounds for believing that there is in force in the place of transfer a law which is substantially similar to or serves the same purpose as the PDPO;
- (c) the data subject has consented in writing to the international transfer;
- (d) the data user has reasonable grounds for believing, in all the circumstances of the case –
 - (i) the transfer is for the avoidance or mitigation of adverse action against the data subject,
 - (ii) it is not practicable to obtain the consent in writing of the data subject to that transfer, and
 - (iii) if it was practicable to obtain such consent, the data subject would give it;

3 See the discussion at <<https://www.legco.gov.hk/yr16-17/english/panels/ca/papers/ca20170515cb2-1368-3-e.pdf>> (accessed 20 March 2018), at para 4.

- (e) the data is exempted from data protection principle 3 (*ie*, use limitation) under Part 8 of the PDPO; or
- (f) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not in that place, be collected, held, processed or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under the PDPO.

17 In December 2014, the PCPD published a guidance note entitled “Guidance on Personal Data Protection in Cross-border Data Transfer”⁴ (“International Transfer Guidance”). The PCPD acknowledges in the International Transfer Guidance that section 33 of the PDPO is not yet in force but the guidance stands as a practical guide for data users to prepare for the implementation of that section and more generally the International Transfer Guidance serves as encouragement for data users to adopt the practices recommended as part of their corporate governance responsibility to protect personal data. The International Transfer Guidance includes a recommended model form of contract which would serve as one of the methods for reliance on the exception highlighted in (f) above, *ie*, the data user’s reasonable precautions and due diligence taken towards ensuring that the transferred personal data will be processed in accordance with the PDPO in the jurisdiction of transfer.

18 There have been no regulations or subsidiary legislation issued under the PDPO. The PDPO does permit the PCPD to from time to time approve and issue codes of practice. Codes of practice do not in themselves have the force of law in Hong Kong, but failure to observe any provision of a code of practice approved by the PCPD raises a legal presumption that the relevant provision of the PDPO has been breached in the absence of evidence of compliance.

19 The PCPD has approved and issued three codes of practice, relating to: (a) the collection and processing of identity card numbers and other personal identifiers; (b) the collection and processing of consumer credit data; and (c) data protection aspects of human resources

4 <https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_cross_border_e.pdf> (accessed 20 March 2018).

management.⁵ Separately, the PCPD may issue guidelines indicating how the PCPD would perform his functions or exercise his powers under the PDPO.

20 Given the controversies, the Government of the Hong Kong SAR has engaged a consultant in conducting a business impact assessment on the implementation of section 33.⁶ The consultant's initial findings were discussed during a meeting of the Legislative Council Panel on Constitutional Affairs on 15 May 2017. The report is yet to be released. The Government will consider the report and decide the way forward in this matter, noting that further study into the potential business impacts of section 33 was needed.

ii Specific provisions in financial sector

21 All organisations that are “data users” within the meaning of the PDPO, irrespective of their activity or field of industry, are subject to the PDPO, which stands as comprehensive data protection legislation. There are therefore no other international data transfer restrictions imposed by laws and regulations other than section 33.

22 However, the Monetary Authority (“HKMA”), which has responsibility for regulating authorised institutions licensed under the Banking Ordinance,⁷ expects that authorised institutions will give specific notice to customers of significant outsourcing initiatives, particularly if the outsourcing is to an overseas jurisdiction.⁸ It also expects these institutions to address the risks arising from overseas outsourcing, taking into account relevant aspects of an overseas country (eg, legal system, regulatory regime and the sophistication of the technology and infrastructure). Interestingly, the HKMA advises these

5 <https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/code.html> (accessed 20 March 2018).

6 <<http://www.legco.gov.hk/yr16-17/english/panels/ca/papers/ca20170515cb2-1368-3-e.pdf>> (accessed 20 March 2018).

7 Cap 155.

8 The Monetary Authority, *Supervisory Policy Manual SA-2 Outsourcing V.1 – 28.12.01* at para 2.5.3 <<http://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf>> (accessed 20 March 2018).

institutions, in relation to overseas outsourcing, to take account of the provisions of section 33 of the PDPO and the potential impact on their plans in respect of overseas outsourcing, “although §33 has not yet come into operation”.⁹

23 There is no specific penalty for any failure to give specific notice to customers of significant outsourcing initiatives, but the HKMA could consider the failure in the context of assessing the institution’s compliance with its authorisation criteria and it would likely issue some form of direction to remedy it.

iii Constitutional protections

24 Hong Kong’s constitutional document is the Basic Law of the Hong Kong Special Administrative Region of the People’s Republic of China (“Basic Law”),¹⁰ a national law of the PRC.

- (a) Articles 28 to 30 of the Basic Law provide a basic framework within which individual rights to privacy are protected at a constitutional level.
- (b) Article 28 prescribes a general freedom from arbitrary or unlawful search of the body.
- (c) Article 29 extends this freedom to individuals’ homes or other premises.
- (d) Article 30 provides that the freedom and privacy of communications by Hong Kong residents shall be protected by law, subject to relevant authorities being permitted to inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences.
- (e) Article 39 provides that the provisions of the International Covenant on Civil and Political Rights (“ICCPR”), *etc.*, shall remain in force after the handover of Hong Kong. Also, the right to privacy as stipulated in the ICCPR was incorporated

9 The Monetary Authority, *Supervisory Policy Manual SA-2 Outsourcing V.1 – 28.12.01* at para 2.9.1 <<http://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf>> (accessed 20 March 2018).

10 <<http://www.basiclaw.gov.hk/en/basiclawtext/>> (accessed 20 March 2018).

into law by way of the Hong Kong Bill of Rights Ordinance¹¹ (“1991 Bill of Rights Ordinance”).

- (f) Article 14 of the Hong Kong Bill of Rights Ordinance provides the protection of privacy, family, home, correspondence, honour and reputation (which is a replica of Article 17 of the ICCPR).

Hence, a constitutional framework of privacy law is already in place in Hong Kong.

iv *International engagement*

25 When the UK ratified the ICCPR in 1976, it did so for itself and extended it to its then colony, Hong Kong, with certain reservations. The ICCPR was incorporated into the law of Hong Kong through the 1991 Bill of Rights Ordinance.

26 Hong Kong has not negotiated nor signed any bilateral or multilateral free trade agreement with other jurisdictions covering transfers of personal data between them.

27 Hong Kong, China is an Asia-Pacific Economic Cooperation (“APEC”) member economy. The PCPD, a participant of the APEC Cross-border Privacy Enforcement Arrangement (“CPEA”), provides support and advice to the Government of the Hong Kong SAR in the APEC discussions relating to personal data protection. The Government of Hong Kong has not yet joined or lodged a Notice of Intent to participate in the APEC Cross-border Privacy Rules (“CBPR”) System, but is currently considering whether to apply to join.

28 Hong Kong is not uniquely impacted by the pending implementation of the European General Data Protection Regulation (“GDPR”). The GDPR will extend European data protection laws to organisations offering goods or services to persons in the European Union (“EU”) or monitoring the behaviour of persons in the EU, irrespective of whether or not that organisation is established in the EU through a physical presence or equipment located there. This means that

11 Cap 383, 1991.

there will be Hong Kong organisations not currently subject to EU data protection law that will become subject to it with the implementation of the GDPR. According to the information available in the EU Commission's website, the EU is Hong Kong's second major trading partner after China.

v *Role of PCPD for personal data in international transfers*

29 The PCPD has statutory responsibility for administering the PDPO.¹² As discussed above, international data transfer restrictions are currently not in force under the PDPO, but the PCPD has published the International Transfer Guidance as a voluntary best practice guide for organisations undertaking international transfers of personal data.¹³ If section 33 were brought into force as drafted, the PCPD would be empowered to publish a notice in the *Gazette* stating certain jurisdictions having been determined to have a law substantially similar to or serving the same purpose as the PDPO.

30 The PCPD is an Accredited Member of the International Conference of Data Protection and Privacy Commissioners.

C DEFAULT POSITION, SCOPE AND TERRITORIAL EFFECT

i *Default position*

31 As outlined in more detail above, international transfers are permitted, pending the introduction of an international transfer restriction that is not yet in force. The PCPD's International Transfer Guidance provides recommended best practice measures for administering international transfers of personal data, but these are not binding.

12 <<https://www.pcpd.org.hk/>> (accessed 20 March 2018). The PCPD's office is located at 12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong. E-mail enquiries may be made to <enquiry@pcpd.org.hk>.

13 <https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_cross_border_e.pdf> <https://www.pcpd.org.hk/>.

ii *Scope of restriction*

32 If section 33 were brought into force as currently drafted, it would apply to: (a) transfers of personal data from Hong Kong to a place outside Hong Kong; and (b) transfers of personal data between two other jurisdictions where the transfer is controlled by a Hong Kong data user (*ie*, a person who either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data) (section 33(1)).

33 The PDPO governs personal data privacy protection of individuals in all sectors (public and private). If section 33 were brought into force as currently drafted, therefore, it would apply to all persons being “data users”, being persons who either alone or jointly or in common with other persons, control the collection, holding, processing or use of the data, irrespective of their sector or field of activity.

34 If section 33 were brought into force as currently drafted, it would apply to all personal data, irrespective of their sensitivity; in fact, the PDPO does not include a concept of “sensitive personal data”. The concept of personal data is, however, very broad. For example, recent enforcement cases have also confirmed that the PDPO applies to personal data that are publicly available.¹⁴

35 Section 33 would apply to “personal data” being data relating directly or indirectly to a living individual from which it is practicable for the identity of the individual to be directly or indirectly ascertained, where such data are in a form in which access to or processing of the data is practicable. The PDPO does not expressly deal with anonymised, pseudonymised or encrypted personal data, but any data that fail to satisfy the definition of “personal data” are not covered by the PDPO. It is the PCPD’s regulatory stance that encryption alone is not sufficient to exclude the data from the purview of the PDPO. The PCPD has

14 See <https://www.pcpd.org.hk/english/enforcement/decisions/files/AAB_54_2014.pdf> (accessed 20 March 2018). See also Privacy Commissioner for Personal Data, “Guidance on Use of Personal Data Obtained from the Public Domain” found at <https://www.pcpd.org.hk/english/publications/files/GN_public_domain_e.pdf> (accessed 20 March 2018).

published a guidance note “Guidance on Personal Data Erasure and Anonymisation”¹⁵ that recognises that personal data may be processed in such a way that the data are no longer personal data. Due to the risk of re-identification and big data analytics, there are concerns as to whether it will still be possible to genuinely and effectively anonymise data.

36 If section 33 were brought into force as currently drafted, it would apply to all international transfers, irrespective of the nature of the recipients, sector or scale of processing: the PDPO regulates “data users”, the definition of which broadly corresponds to the “data controller” concept under European data protection law. “Data processors” are not directly regulated under the PDPO; they are, however, made subject to indirect obligations (pursuant to data protection principles 2(3) and 4(2) in the PDPO) in which the data users appointing them are required to adopt contractual or other means to (a) prevent data transferred to data processors from being kept longer than is necessary for processing, and (b) prevent unauthorised or accidental access, processing, erasure, loss or use of the data.

37 If section 33 were brought into force as currently drafted, it would apply to data imported by a Hong Kong user, irrespective of the data subject’s nationality or of the location where the data had originally been collected.

38 If section 33 were brought into force as currently drafted, the relevant provision would not define the meaning of “transfer” or exempt any form of “transfer” (*eg*, under an outsourcing exemption). Nonetheless, in the International Transfer Guidance, the PCPD has adopted the stance that section 33 did not apply, for example, “when a telecommunication service provider transmits personal data for other data users”, if the telecommunication service provider was not a “data user” and did not transmit the data for its own purpose.

15 <https://www.pcpd.org.hk/english/publications/files/erasure_e.pdf> (accessed 20 March 2018).

D DATA LOCALISATION

39 No data localisation laws apply in Hong Kong.

E LEGAL BASIS AND DATA TRANSFER MECHANISMS

i *Preliminary issues*

40 The fact that different jurisdictions have different rules for international transfers of personal data across the region poses significant challenges for multinational businesses based in or hubbed in Hong Kong. The absence of unifying standards means that in practice, some jurisdictions have data localisation, some require opt-in consents, some enable other means of achieving compliant international transfers, such as reliance on “white lists” or the use of contract terms (the substance of which may also vary from jurisdiction to jurisdiction). For many organisations these points of difference generate uncertainty and inefficiency, without it necessarily being the case that the data subjects’ interests are advanced through, for example, improved data security or regulatory oversight. Therefore, the latest developments are jurisdictions looking for developing interoperability between different systems.

41 Financial services sector businesses in particular are seeking compatible transfer instruments. Given the sensitivity of the personal data that they process and the stringency of their regulatory environment, financial institutions are amongst the most likely to have implemented data transfer agreements that would benefit from a more harmonised approach across the region. However, the pervasive use of mobile and cloud-based technologies, and the general push by businesses across a range of sectors towards more intensive use of data means that the challenge of managing cross-border transfers is increasingly a universal one.

42 In general, it is important to note that whilst international transfers of personal data are not currently restricted under the PDPO, a transfer of personal data from one party to another (whether within Hong Kong or cross-border) is regulated under the PDPO and so, in practice, data subject notifications/consents must reflect the fact of transfers to third parties, and contracts with those third parties must describe the nature of

the transfer, the purposes for which the data may be used or made subject to further onward transfer, secure processing measures and other compliance matters under the PDPO. Apart from PDPO compliance, there are good business reasons to have an appropriate contract in place covering transfers of personal data or other non-contractual measures to protect personal data transferred overseas.

43 In the same vein, transfers to a data processor are regulated under the PDPO, whether the data crosses borders or not. Data users transferring personal data to a data processor must adopt contractual or other means to: (a) prevent any personal data from being kept by the data processor longer than is necessary for the processing of the data; and (b) prevent unauthorised or accidental access, processing, erasure, loss or use. The PDPO prescribes that the data user remains liable in case of a breach by the data processor, whether the transfer from the user to the processor is cross-border or not.

44 The PCPD has not endorsed any specific self-regulation or self-certification. In February 2014, however, the PCPD launched a voluntary accountability model called “Privacy Management Programme” (“PMP”) supported by the publication of a best practice guide.¹⁶ PMP relates to data protection compliance generally and not specifically to international transfers of personal data.

ii *No notification to Privacy Commissioner*

45 If section 33 were brought into force as currently drafted, exports would not require any notification to or approval by any regulator.

iii *“Adequacy findings” and white lists*

46 If section 33 were brought into force as currently drafted, it would make provision for the PCPD to publish a “white list” of comparable jurisdictions, to which international transfers could be made without

16 <https://www.pcpd.org.hk/pmp/files/PMP_guide_e.pdf> (accessed 20 March 2018).

consent or other compliance requirements relating to the transfer being fulfilled. The PDPO, on the other hand, does not explicitly empower the PCPD to publish a “black list”.

47 If section 33 were brought into force as currently drafted, it would support data users making their own assessment of whether or not there are reasonable grounds for believing that there is in force in the place of transfer a law which is substantially similar to or serves the same purpose as the PDPO. In the International Transfer Guidance, however, the PCPD articulated an expectation that the self-assessment would be carried out only in respect of transfer jurisdictions not already assessed and rejected by the PCPD as “white list” candidates, meaning that there could effectively be a “black list” if section 33 were administered as contemplated in the guidance. The law itself does not list the substantive standards for establishing comparable data protection standards. In the International Transfer Guidance, the PCPD has suggested various factors for data users’ consideration when conducting the assessment of the comparable standard.

48 If section 33 were brought into force as currently drafted, it would not expressly contemplate sectoral adequacy, but instead invites the PCPD to consider if a “place” has a law substantially similar to or serving the same purpose as the PDPO. Nevertheless, the PCPD may consider if compliance with a highly regulated industry’s code of practice may fall within the exception to the restriction on international transfers of personal data (see above): “the data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not in that place, be collected, held, processed or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under this Ordinance” (section 33(2)(f)).

49 Whilst no cost/benefit analysis of “adequacy decisions” and “white lists” has yet officially been done in the jurisdiction, in 2013 the PCPD had commissioned a consultancy study to complete a survey of 50 jurisdictions and come up with a white list of places which has in force a data protection law which is substantially similar to, or serves the same purpose as the Ordinance, and had delivered the report to the

Government of Hong Kong for comment.¹⁷ However, the “white list” has not been published.

iv *Consent as exception to existence of privacy safeguards overseas*

50 If section 33 were brought into force as currently drafted, data subjects’ consent alone should be a sufficient legal basis for transfer of personal data to a place outside Hong Kong. The data subject’s consent is required to be in writing (section 33(2)(b)). The PCPD has provided guidance in the International Transfer Guidance for obtaining consent from data subjects for the international transfer. In particular, consent should be voluntarily given and not been withdrawn by the data subject in writing.

v *Other one-off exceptions*

51 The performance of a contract in the interest of the individual is mentioned in the International Transfer Guidance as an example of the exception to the transfer restriction in section 33(2)(d), which provides that “the user has reasonable grounds for believing that the transfer is for the avoidance or mitigation of adverse action against the data subject, it is not practicable to obtain the consent in writing of the data subject to that transfer, but if it was practicable, such consent would be given”. The PCPD has specified that this exemption from consent would have a narrow application, and that data users have to prove their belief in the context of the relevant circumstances surrounding the transfer.

vi *Contracts*

52 If section 33 were brought into force as currently drafted, it would not be compulsory for a Hong Kong data exporter to conclude a contract

17 Privacy Commissioner for Personal Data, Media Statements, 23 January 2014, “The Year 2013 Saw a 48% Increase in Privacy Complaints” <https://www.pcpd.org.hk/english/news_events/media_statements/press_20140123a.html> (accessed 20 March 2018).

with an importer, given the other means available of achieving compliance with that section. Section 33(2)(f) requires a data user who wishes to transfer personal data outside Hong Kong to take all reasonable precautions and exercise all due diligence to ensure that the data will not, in that place, be collected, held, processed or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under the PDPO. In this connection, the PCPD has provided in the International Transfer Guidance the Recommended Model Clauses for voluntary adoption and adaption by parties in a data transfer agreement for compliance with the “Due Diligence Requirements”.

53 Whether or not a data user elects to use the Recommended Model Clauses, in practice a form of contract will need to be used, given that a data user must put in place a contract (or other means) to ensure that the requirements for transfer of personal data discussed above¹⁸ (whether or not cross-border) are met.

54 The Contracts (Rights of Third Parties) Ordinance¹⁹ provides for third-party rights to enforce contractual terms in certain circumstances, which could conceivably be deployed in such a way as to give data subjects direct rights of enforcement against data importers under cross-border transfer agreements settled under Hong Kong law. The third party’s right is expressed as optional in the Recommended Model Clauses for data transfer agreement as attached to the International Transfer Guidance. There is no requirement under section 33 that data subjects be given direct rights of enforcement under cross-border transfer agreements.

vii CBPRs

55 Hong Kong has not joined or lodged a Notice of Intent to participate in the APEC CBPR System.

18 See para 36 above.

19 Cap 623.

viii *Certification, trustmarks and privacy seals*

56 Hong Kong has not implemented any privacy certification schemes, trustmarks or privacy seals. However, it is conceivable that if section 33 were brought into force, the PCPD could consider if certification mechanisms, privacy seals and trustmarks delivered in a third country would fall within the exception to the restriction on international transfers of personal data: “the data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not in that place, be collected, held, processed or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under the this Ordinance” (section 33(2)(f)).

ix *Other data transfer instruments (binding corporate rules, ISO certification, etc)*

57 As explained on page 7 of the International Transfer Guidance, a data user may take the following approaches in order to satisfy the conditions for international transfers under section 33 of the PDPO:

- (a) using enforceable contract clauses;
- (b) using non-contractual oversight and auditing mechanisms to monitor transferees; and
- (c) adopting internal safeguards, policy and procedures for intra-group transfers.

F ENFORCEMENT OF SECTION 33 PDPO AND INTERNATIONAL CO-OPERATION BETWEEN PCPD AND OTHER PRIVACY ENFORCEMENT AUTHORITIES

i *Enforcement of cross-border transfer restrictions*

58 Section 33 of the PDPO imposes a restriction on international transfers of personal data, but this provision has not yet been brought into effect and a notice in the *Government Gazette* would be required in order for this to be the case. If section 33 were brought into force, data users who, without reasonable excuse, contravene section 33 would commit an offence under section 64A of the PDPO, which carries a fine of up to HK\$10,000.

59 The PCPD would also be in a position to issue enforcement notices to data users who have contravened section 33, directing the data users to take remedial action. Non-compliance with an enforcement notice is an offence under the PDPO. The offender is liable on a first conviction (by a magistrate or a court) to a fine of HK\$50,000 and to imprisonment for two years. A daily penalty of HK\$1,000 per day applies if the offence continues after conviction (section 50A).

60 The power to prosecute offences is vested in the police and the Department of Justice, and the power to impose penalties is vested in the magistrates and the courts. However, as section 33 of the Ordinance is not yet in operation, there has been no enforcement action taken by the PCPD for the sole reason that personal data was transferred to a place outside Hong Kong. The PCPD has not published an enforcement policy on data transfer requirements.

ii Co-operation with foreign PEAs

61 The PCPD was set up to enforce the PDPO. The primary objective of the PCPD is to ensure that its regulatory guidance and decisions are in line with the requirements under the PDPO. At the same time, to the extent not incompatible with the requirements of the PDPO, the PCPD also strives to keep in line with regional and international practices in our regulatory guidance and decision-making process. The PCPD has been actively monitoring the regulatory guidance and decisions of other privacy enforcement authorities (“PEAs”) with a view to maintaining consistency with the international practice.

62 The PDPO further includes provisions that enable the PCPD to develop operational co-operation with the PEAs in other jurisdictions. Specifically, section 8(1)(g) of the PDPO states that the PCPD shall:

... liaise and co-operate with any person in any place outside Hong Kong—

- (i) performing in that place any functions which, in the opinion of the PCPD, are similar (whether in whole or in part) to any of the PCPD’s functions under this Ordinance; and

- (ii) in respect of matters of mutual interest concerning the privacy of individuals in relation to personal data ...

63 Section 8(2)(b) of the PDPO further provides that the PCPD may do “all such things as are necessary for, or incidental or conducive to, the better performance of his functions”, including entering into agreement or other obligation.

a Bilateral arrangements

64 The PCPD has signed a memorandum of understanding (“MOU”) for Cooperative Research on Personal Data Protection with the Korea Information Security Agency (“KISA”) in November 2002, to co-operate in conducting research on personal data privacy and sharing education and training programmes. The MOU is non-binding but acts as an expression of both parties’ genuine interest to explore opportunities for future co-operation.

b Multilateral arrangements for cross-border co-operation

65 The PCPD is party to several multilateral arrangements for cross-border co-operation, namely:

- (a) the APEC Cross-border Privacy Enforcement Arrangement (“CPEA”);
- (b) the International Conference for Data Protection and Privacy Commissioners (“ICDPPC”), including its Global Cross Border Enforcement Cooperation Arrangement;
- (c) the Global Privacy Enforcement Network (“GPEN”), which is an informal network of PEAs established for general knowledge sharing and information exchange to address cross-border challenges;
- (d) the Asia Pacific Privacy Authorities (“APPA”); and
- (e) the International Working Group on Data Protection in Telecommunications (also known as the “Berlin Group”).

The PCPD does not participate in the Unsolicited Communications Enforcement Network (“UCENet”) or the APEC CBPR framework.

iii *International enforcement by PCPD*

66 The PDPO allows disclosure of information concerning investigations of complaints but not a transfer of the complaints to a foreign authority as such. The law also allows the PCPD to do such things required including seeking assistance from the overseas PEAs when handling complaints made under the PDPO.

67 Section 46 of the PDPO empowers the PCPD to disclose matters to an authority outside of Hong Kong, either for the purposes of performing its functions or exercising its powers under the PDPO or for the purpose of enabling or assisting that foreign authority. There are important conditions attached to these provisions. In particular, the PCPD must ensure that the co-operating authority has undertaken to be bound by the PCPD's secrecy requirements. Disclosures in support of assisting a foreign authority may only be made if the PCPD is of the opinion that the foreign jurisdiction in question has a law in force that is substantially similar to or serves the same purpose as the PDPO. Disclosures in support of the PCPD performing its function or exercising its powers under the PDPO may be made if one of a longer set of conditions is met, such as relevant data subjects having consented to the disclosure or one of the exemptions to the use limitation requirement under the PDPO applies (if for example, the disclosure relates to the investigation of a crime under Hong Kong law).

68 The PCPD has been involved in co-ordinated efforts involving authorities from many countries over the past years, such as the GPEN Sweep. For instance, in May 2013 and as part of the GPEN Sweep initiative, the PCPD conducted a study into the privacy transparency of mobile apps. It conducted a study on the 60 most popular apps developed by Hong Kong entities and found that their privacy policies were generally inadequate.²⁰

20 This led the Privacy Commissioner for Personal Data to publish the "2014 Study Report on the Privacy Policy Transparency ('2014 Sweep Initiative') of Smartphone Applications", with recommendations attached, in December 2014 <https://www.pcpd.org.hk/english/resources_centre/publications/surveys/files/sweep2014_e.pdf> (accessed 20 March 2018).

69 The PCPD has also engaged in cross-border enforcement co-operation with overseas PEAs, although it has never undertaken a joint investigation with a PEA from another country. For instance, on occasion it has provided assistance to an investigation being undertaken by a PEA from another country, referred a complaint to a PEA overseas, and received complaint referrals from a PEA in another country.

70 At the time of writing, the PCPD has not yet taken an enforcement action jointly with one of its foreign counterparts or issued common findings against a foreign controller (“data user” under the PDPO) based in multiple jurisdictions.

Jurisdictional Report

INDIA

Reporters: **Amber Sinha**

Senior Programme Manager, The Centre for Internet & Society

Elonnai Hickok

Chief Operating Officer, The Centre for Internet & Society

A BACKGROUND INFORMATION

1 India currently does not have a data protection legislation. However, the painstaking process of passing a comprehensive Data Protection Act was recently reactivated by the Indian government, who said in August 2017 that it is “cognizant of the growing importance of data protection in India. The need to ensure growth of the digital economy while keeping personal data of citizens secure and protected is of utmost importance”.¹

2 Several factors have played a role in this evolution.

3 The first factor is, without contest, the judgment of the Supreme Court of India in *Puttaswamy v Union of India*² (“*Puttaswamy*”), which has read privacy (including privacy of information) into the fundamental right to life and liberty, as well as the entire Part III (“Fundamental Rights”) in the Indian Constitution. An in-depth analysis of this landmark decision is available on the website of the Centre for Internet and Society.³

1 Office Memorandum No 3(6)j2017-CLES of 31 August 2017 of the Ministry of Electronics & Information Technology on the Constitution of a Committee of Experts to deliberate on a data protection framework for India – <http://www.meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf> (accessed 26 March 2018).

2 Available at <<https://indiankanoon.org/doc/91938676/>> (accessed 26 March 2018).

3 <<https://cis-india.org/internet-governance/blog/the-fundamental-right-to-privacy-an-analysis>> (accessed 26 March 2018).

4 In this judgment, privacy has been held as both a negative and a positive right, meaning that not only does it restrain the State from committing an intrusion upon the life and personal liberty of a citizen, it also imposes an obligation on the State to take all necessary measures to protect the privacy of the individual. This judgment is significant in its recognition of the threats to informational privacy in the digital age, as it considers ubiquitous data collection in a networked society, digital trails of people's online activities, algorithmic analyses of data and metadata collected, the relative invisibility of access and processing of electronic data, the recombinant nature of data and the building of profiles through data aggregation. This is the first instance of the recognition of threats of privacy in the age of big data and algorithmic decision making by the Supreme Court and differences between volunteered data, observed data and inferred data. These observations would be of great value in future cases where the extent and nature of data collections and processing may be considered before the court.⁴ Furthermore, the judgment depicts many facets of privacy, but the idea of informed consent as central to informational privacy is a key thread that runs across the different opinions in the judgment. This point is particularly relevant to the current debates regarding the nature of data protection law that India should formulate and adopt.

5 It is very likely, therefore, "that, in order to protect the constitutionality of other legislation and practices, the Indian government will now have to legislate comprehensively to protect privacy in relation to both the public and private sectors in India".⁵

6 The second factor is that achieving greater clarity on international data transfer procedures and alignment with international standards and laws could provide a great fillip for the data processing industry in India. In this context, India has a renewed ambition to achieve adequacy status by European law. Conversations with government actors in India, the European Commission as well as news items suggest that there is a great

4 <<https://cis-india.org/internet-governance/blog/the-fundamental-right-to-privacy-an-analysis>> (accessed 26 March 2018).

5 Graham Greenleaf, "Privacy in South Asian (SAARC) States: Reasons for Optimism" (2017) 149 *Privacy Laws & Business International Report* 18.

degree of geopolitical and economic interest from both parties in granting India an adequacy status (see below).

7 Thirdly, considering that many Asian countries have attempted to implement data localisation policies in order to benefit their domestic technology sector and industries, there is a degree of fragmentation with regard to data flows across borders in the region. The challenges extend to limiting the level of data localisation practiced by countries, and instituting interoperability between countries – which will benefit all the countries by promoting regional free-flow of information that will help in enforcing security measures, business development and technological innovation. For example, the Trans-Pacific Partnership looks to implement regulations that limit data localisation, prohibit digital custom duties and promote cross-border data flows in order to reap the benefits of free and unhindered flow of information.

8 The current discussions on the Data Protection Bill, therefore, should take into account these multiple parameters.

B LEGAL FRAMEWORK OF INTERNATIONAL DATA TRANSFERS IN INDIA

9 As stated above, India currently does not have a data protection legislation, and Indian laws do not comprehensively address the issues of international data transfers. Some regulations apply to transfers of electronic data by body corporates, which apply to both domestic and international parties. Further, some sectoral laws address the international transfer of specific categories of data including communications data and financial data. These policies are covered in more detail below.

i International data transfers and the pending draft Data Protection Bill

10 In August 2017, India's Ministry of Electronics and Information Technology ("MeitY") constituted the Committee of Experts on a Data Protection Framework for India under a former judge of the Supreme Court, Justice B N Srikrishna ("the Committee" or "Justice Srikrishna

Committee”). According to the Ministry’s order,⁶ the terms of reference of the Committee were:

- (a) to study various issues relating to data protection in India; and
- (b) to make specific suggestions for consideration of the Central Government on principles to be considered for data protection in India and suggest a draft Data Protection Bill.

11 The Supreme Court in *Puttaswamy* took cognisance of the fact and stated:⁷

Since the government has initiated the process of reviewing the entire area of data protection, it would be appropriate to leave the matter for expert determination so that a robust regime for the protection of data is put into place. We expect that the Union government shall follow up on its decision by taking all necessary and proper steps.

12 The Committee released a white paper on 27 November 2017, articulating provisional views on various issues relevant to the framing of a data protection law, including the principles and institutional frameworks necessary for cross-border data flow.⁸

13 Along with this, the Telecom Regulatory Authority of India (“TRAI”) also issued a consultation paper on data protection which would serve as a point of reference for drafting the Bill.⁹ The Government had earlier stated that a data protection law would be adopted before the end of 2017. However, as of now, as the Committee has only begun deliberations, it is unclear as to the expected timeline for the drafting and adoption of the law.

6 <http://www.meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf> (accessed 26 March 2018).

7 *Puttaswamy v Union of India*, available at <<https://indiankanoon.org/doc/91938676/>> (accessed 26 March 2018).

8 “White Paper on Data Protection Framework for India” <http://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf> (accessed 26 March 2018).

9 “Consultation No 09/2017 on Privacy, Security and Ownership of the Data in the Telecom Sector” <http://www.trai.gov.in/sites/default/files/Consultation_Paper%20_on_Privacy_Security_ownership_of_data_09082017.pdf> (accessed 26 March 2018).

14 Prior to the forming of this Committee there had been draft legislation released in 2011¹⁰ and 2014.¹¹ However, neither of the Bills were tabled in Parliament for consideration. Additionally, the 2014 Bill formulated by the Government does not address the issue of international data transfers. Interestingly, the 2012 Report of the Group of Experts on Privacy, which recommends a privacy framework for India and defines nine national privacy principles, also does not address cross-border transfer of data.¹² In contrast, the 2011 Bill contained a provision on transborder data flows of personal data (section 22). More significantly, the White Paper released by the Justice Srikrishna Committee deals with the issue of cross-border data protection and asks numerous questions for consultation related to it. The paper recognises that providing strong rules to protect cross-border data flows is vital for small and medium-sized enterprises or “SMEs”, consumers and multinational businesses. The paper opines that the adequacy test is particularly beneficial and the proposed data protection authority should be able to determine it to ensure a smooth two-way flow of information, critical to a digital economy. The paper seeks views and public consultation on issues such as specific provisions facilitating cross-border transfer of data and cross-border flow of data particularly sensitive personal data.

15 Today, therefore, no comprehensive provision exists in Indian law that regulates the transfer of personal data outside of India.

16 Only the governance of electronic personal and sensitive personal data is partially addressed under section 43A¹³ of the Information Technology Act, as amended in 2008 (“IT Act”), and the associated Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 of the IT Act.

10 <<https://cis-india.org/internet-governance/draft-bill-on-right-to-privacy>> (accessed 26 March 2018).

11 <<http://164.100.47.4/Bills/Texts/RSBill/Texts/asintroduced/data%20-E.pdf>> (accessed 26 March 2018).

12 <http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf> (accessed 26 March 2018).

13 Information and Technology Act, 2008 s 43A (available at <<http://www.eprocurement.gov.in/news/Act2008.pdf>> (accessed 26 March 2018)).

17 Section 43A of the IT Act (“Compensation for failure to protect data”) provides that:

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

18 In its explanatory paragraph (ii), section 43A further provides that “reasonable security practices and procedures” may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit. On that basis, on 11 April 2011, the Ministry of Communications and Information Technology of the Central Government adopted the Information Technology (Reasonable security practices and procedures and sensitive personal data and information) Rules, 2011 (“the Section 43A Rules”, or “the 2011 Rules”).¹⁴

19 There are no comprehensive provisions dealing with international data transfers in these Rules. Only rule 7 provides that “sensitive personal data or information”, and not all categories of personal data, may be disclosed (whether within or outside India) only if that disclosure is necessary for the performance of the contract with the provider of information, or where the provider has consented to the transfer. The obligations relating to disclosure of sensitive personal data will also apply to third-party processors.¹⁵ This rule applies to both domestic and international transfers.

ii *Restrictions on international data transfers in specific sectors*

20 Other requirements related to cross-border sharing of data that can be found in sectoral law and policy. These include restrictions on

14 <<http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf>> (accessed 26 March 2018).

15 See para 59 below.

transferring certain categories of data outside of India, which take the form of data localisation obligations and will be studied below.

21 For example, the Unified Access Services Licence (“UASL”), and Unified License (“UL”) are the two sets of regulations under the Department of Telecommunications. Clause 39.23(viii) of the UL states that:¹⁶

The Licensee shall not transfer the following to any person/place outside India:-

- (a) any accounting information relating to subscriber (except for international roaming/billing) (Note: it does not restrict a statutorily required disclosure of financial nature);
- (b) user information (except pertaining to foreign subscribers using Indian Operator’s network while roaming and IPLC subscribers) ...

The same is also stated in clause 41.20.viii of the UASL.¹⁷

22 Furthermore, recently, regulators in India have exhibited an interest in understanding the issues of cross-border data transfers to formulate policies. These include the Consultation Paper on Cloud Computing issued on 10 June 2016,¹⁸ the Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector issued on 9 August 2016¹⁹ by TRAI and the Consultation Paper on P2P Lending by the Reserve Bank of India issued in April 2016.²⁰ Any policies drafted on the basis of these papers could have an impact on cross-border flow of data. Most significantly, the White Paper released by the Justice Sri Krishna Committee definitely exhibits an inclination to address the issues regarding cross-border data flow in its recommendations.

16 <http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf> (accessed 26 March 2018).

17 <<http://www.dot.gov.in/sites/default/files/UAS%20license-agreement-19-12-2007.pdf?download=1>> (accessed 26 March 2018).

18 <<http://www.trai.gov.in/consultation-paper-cloud-computing-0>> (accessed 26 March 2018).

19 <http://www.trai.gov.in/sites/default/files/Consultation_Paper%20_on_Privacy_Security_ownership_of_data_09082017.pdf> (accessed 26 March 2018).

20 <<https://cis-india.org/raw/rbi-consultation-paper-on-p2p-lending>> (accessed 26 March 2018).

iii *Impact of regional data protection frameworks*

23 India has been an observer to the Asia-Pacific Economic Cooperation (“APEC”) Cross-border Privacy Enforcement Arrangement since November 2011. Since the inception, India has expressed interest to join APEC. In the recent past, there have been increasing reports of the conditions being favourable for India to be a part of APEC, in which case there may be a possibility of it joining the Cross-Border Privacy Rules System.²¹

24 India is also a member of the Association of Southeast Asian Nations (“ASEAN”) Plus Six group. So far, there has been no clear avowal of the ASEAN Framework on Personal Data Protection by India.

25 As previously mentioned, for now India has not been recognised by the European Union (“EU”) as offering an adequate level of protection in the application of Article 25(6) of Directive 95/46/EC. News items and conversations with government actors in India as well as those close to the European Commission suggest that there is a great degree of geopolitical and economic interest from both parties in granting India an adequacy status. However, in the absence of a robust data protection legislation in India, past analysis undertaken by CRIDS, the Research Centre in Information, Law and Society based in Namur (Belgium), in contract with the Directorate General Justice, Freedom and Security of the European Commission have found the Indian regime to be inadequate.²² There is no sign that this evaluation would change with the requirements found under the European General Data Protection Regulation (“GDPR”) as well as the opinions released by the Article 29 Working Party. As a note, bodies working on data protection in India

21 <<https://economictimes.indiatimes.com/news/economy/foreign-trade/conditions-for-indias-apec-membership-more-favourable-kevin-rudd/articleshow/51221745.cms>> (accessed 26 March 2018).

22 CRID-University of Namur, “First Analysis of the Personal Data Protection Law in India” <<https://researchportal.unamur.be/en/publications/first-analysis-of-the-personal-data-protection-law-in-india-final>> (accessed 26 March 2018).

have taken a contrary position, and have published analysis arguing that India should qualify as providing adequate protection.²³

26 India has been seeking this status for a number of years through trade agreements with the EU,²⁴ as the lack of such a status leads to higher operating costs for Indian companies handling EU data and impacts their ability to compete for business from European data controllers. Indeed, 30% of India's US\$100b information technology ("IT") and business process outsourcing industry comes from customers based in the European market.²⁵ In 2012, the Data Security Council of India estimated that the outsourcing business can further grow by US\$50b per annum if India is recognised as a "data secure" destination by the EU.²⁶ This is even more important as India, which has a strong track record of performing low-end data processing in the EU, desires to move up the value chain into more sophisticated outsourced work in sectors such as healthcare, clinical research and engineering design.²⁷

27 Experts, civil society and industry have predicted that being compliant with the GDPR is critical and an opportunity for the Indian IT industry,²⁸ but will be difficult and expensive given new requirements

23 Data Security Council of India, "EU Adequacy Assessment of India" (7 January 2012) <https://www.dsci.in/sites/default/files/White_Paper_EU_Adequacy_Assessment_of_India.pdf> (accessed 26 March 2018).

24 Lakshman, Sriram, "EU had offered India gradual, asymmetric elimination of tariffs" (*The Hindu*, 26 April 2016) <<http://www.thehindu.com/business/Industry/eu-had-offered-india-gradual-asymmetric-elimination-of-tariffs/article8524692.ece>> (accessed 26 March 2018).

25 Tim Wright, "India Demands EU Data Secure Nation Status But Still Lacks Robust Data Protection Laws" <www.sourcingfocus.com/site/opinionsitem/5308> (accessed 26 March 2018).

26 Dr Dinoj Kumar Upadhyay, "India-EU FTA: Building New Synergies" (Indian Council of World Affairs, 27 November 2012) <<http://www.icwa.in/pdfs/VPIndiaEUTFA.pdf>> (accessed 26 March 2018).

27 Tim Wright, "India Demands EU Data Secure Nation Status But Still Lacks Robust Data Protection Laws" <www.sourcingfocus.com/site/opinionsitem/5308> (accessed 26 March 2018).

28 <<https://www2.deloitte.com/in/en/pages/risk/articles/eu-gdpr-india.html>> (accessed 26 March 2018).

around data security and data processing.²⁹ Others have predicted that the hefty 4% penalty for data breaches could negatively impact the industry.³⁰ National security concerns have been raised as the regulation will bring IT companies under the scope of EU jurisdiction and it could negatively impact EU companies' decisions to outsource business to India and could stifle innovation.³¹

iv *International data flows and free trade agreements*

28 India has negotiated free trade agreements ("FTAs") with countries such as Japan, South Korea, Singapore, the South Asian Association for Regional Cooperation ("SAARC"), *etc.*³²

29 Some FTAs deal with issues of data protection and related matters as mentioned below.

30 Article 7.21 of the India-Singapore Comprehensive Economic Cooperation Agreement ("ISCECA"), in Chapter 7 "Trade in Services",³³ provides that:

"Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination against the other Party, or a disguised restriction on trade in services, nothing in this Chapter shall be construed to prevent the adoption or enforcement by either Party of measures:

...

29 <<https://www.naavi.org/wp/gdpr-threat-indian-industry/>> (accessed 26 March 2018).

30 <<https://ccgnludelhi.wordpress.com/2016/04/21/the-new-data-protection-directive-and-its-impact-on-india/>> (accessed 26 March 2018).

31 <<http://www.cioandleader.com/article/2017/05/02/india-gets-ready-eu%E2%80%99s-new-data-regime>> (accessed 26 March 2018).

32 <http://commerce.nic.in/trade/international_ta.asp?id=2&trade=i> (accessed 26 March 2018).

33 <<http://commerce.nic.in/trade/ceca/ch7.pdf>> (accessed 26 March 2018). See also Art 7.19 of the India-Singapore Comprehensive Economic Cooperation Agreement.

(c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter including those relating to:

...

(ii) *the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts ...*

[emphasis added]

31 The Japan-India Comprehensive Economic Partnership Agreement contains similar provisions, in relation to the provision of both financial and telecom services.³⁴ In relation to the former, section 6 of Annex 4 to Chapter 6 of the agreement provides that:

Neither Party shall take measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means, or that, subject to importation rules consistent with international agreements, prevent transfers of equipment, where such transfers of information, processing of financial information or transfers of equipment are necessary for the conduct of the ordinary business of a financial service supplier. Nothing in this Section restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of Chapter 6 and related provisions of this Agreement.

32 Regarding the provision of telecommunications services, section 3(4) of Annex 5 to Chapter 6 provides that:

... a Party may take such measures as are necessary to ensure the security and confidentiality of messages or to protect the personal data of users, subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade in services.

33 India's FTA with South Korea also talks about privacy and the protection of personal data as a general exception to rules on the provision of services (Article 6.14). This means that the provisions in the

34 <http://commerce.nic.in/trade/IJCEPA_Basic_Agreement.pdf> (accessed 26 March 2018).

FTA on the trade in services do not apply to any domestic laws in place for “the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts”.³⁵ Specific provisions are to be found in the Chapters of the Agreement on investments (Article 10.7) and trade in telecom services (Article 7.4).

34 The FTA with SAARC also mentions protection of personal data as a general exception on the same lines as the FTA with South Korea.³⁶

35 India and the EU have been negotiating a broad-based trade and investment agreement (“BTIA”) since 2007. It is worth noting that the discussions around EU adequacy status back in 2007 were related to these free trade talks,³⁷ and that receiving adequacy status was a “key demand” of the Indian government during the negotiations. The current discussions around the agreement are now focused on “key outstanding issues that include improved market access for some goods and services, government procurement, geographical indications, sound investment protection rules, and sustainable development”.³⁸ In a recent communication,³⁹ the European Commission has indicated that it will actively engage in discussions on a possible adequacy finding with key trading partners, including India “depending on progress towards the modernisation of its data protection laws”. Indeed, one of the key criteria by which the Commission has announced that it will assess with which third countries a dialogue on adequacy should be pursued is the extent of the EU’s commercial relations with that third country, “including the

35 <<http://commerce.nic.in/trade/INDIA%20KOREA%20CEPA%202009.pdf>> (accessed 26 March 2018).

36 <<http://commerce.nic.in/trade/SAARC%20Agreement%20on%20Trade%20in%20Services%20SATS.pdf>> (accessed 26 March 2018).

37 Pranav Menon, “India-EU Proposed Free Trade Agreement – Issues Surrounding Data Protection and Security” <<https://cis-india.org/a2k/blogs/india-eu-proposed-fta.pdf>> (accessed 26 March 2018).

38 <<http://ec.europa.eu/trade/policy/countries-and-regions/countries/india/>> (accessed 26 March 2018).

39 European Commission, “Protection and Exchange of Personal Data in a Globalised World” (10 January 2017) <<http://europa.eu/rapid/attachment/MEMO-17-15/en/international-transfert-data-08%20final%20.pdf>> (accessed 26 March 2018).

existence of a free trade agreement or ongoing negotiations”, as well as the extent of personal data flows from the EU, reflecting geographical and/or cultural ties. India definitely falls in that category.

36 In all cases, while there are some provisions on data privacy in the FTAs India has signed, until incorporated into law, they do not override any of the national laws governing data protection.

C DATA LOCALISATION

37 There are multiple laws/policies in India that contain data localisation requirements. There is no overarching legislation that categorises data localisation requirements. Some of the legislation look to implement physical storage with data being kept in the country, and some require backups to be kept in the country to protect the user against loss of data and maintaining privacy.

38 These include:

- (a) National Data Sharing and Accessibility Policy (“NDSAP”) Department of Science and Technology (“DST”), 2012,⁴⁰ which advocates for government-processed data or data collected/processed with public funds by authorised agencies, to be stored in data centres that are located physically in the country.⁴¹
- (b) Companies (Accounts) Rules, Ministry of Corporate Affairs (“MCA”), 2014,⁴² which mandates that there should be a backup of financial information and other books or papers of the company stored, on a periodic basis, within the borders of India.⁴³
- (c) The Unified License Agreement, MeitY.⁴⁴

40 <http://www.dst.gov.in/sites/default/files/nsdi_gazette_0.pdf> (accessed 26 March 2018).

41 National Data Sharing and Accessibility Policy at p 10.

42 <http://www.mca.gov.in/Ministry/pdf/NCARules_Chapter9.pdf> (accessed 26 March 2018).

43 Companies (Accounts) Rules, 2014 s 3.

44 <http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf> (accessed 26 March 2018).

- (d) “Guidelines for Government Departments on Contractual Terms Related to Cloud Services”, MeitY, 2015,⁴⁵ which provides that cloud service providers that are looking for government contracts or public funds, must store all such data physically in India.⁴⁶
- (e) Aadhar Regulations (Data Security and Sharing of Information), Unique Identification Authority of India (“UIDAI”), 2016.⁴⁷

39 Proposed policy includes:

- National Telecom M2M Roadmap, MeitY, 2015,⁴⁸ which has not been implemented as of now, but does state that all gateways and application servers serving customers in India and in turn, collecting information, must store it within the country.⁴⁹

40 In some cases, there is no overlap between the data localisation requirements found under the above policies and the data transfer standards found under rule 7 of the Section 43A Rules as policies such as the NDSAP and the “Guidelines for Government Departments on Contractual Terms Related to Cloud Services” address data held by the Government, and do not fall under the Section 43A Rules or the IT Act.

41 On the contrary, the data that fall under the scope of the Unified License Agreement and the Companies (Accounts) Rules, 2014, if it is sensitive personal information, would also fall under the scope of section 43A of the IT Act and the associated Rules.

42 Different localisation principles that have been applied in the private sector can be interpreted in multiple ways, notably whether local and foreign companies are subject to the same obligations.

45 <http://meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf> (accessed 26 March 2018).

46 See para 2.1(d) of the “Guidelines for Government Departments on Contractual Terms Related to Cloud Services” at pp 7–8.

47 <<https://uidai.gov.in/legal-framework/acts/regulations.html>> (accessed 26 March 2018).

48 <<http://www.dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf>> (accessed 26 March 2018).

49 See para 4.2.7(2) of the National Telecom M2M Roadmap at p 40.

43 The NDSAP is silent on local or foreign companies *per se*, as the scope of the legislation is limited to the Government, other ministries, departments, agencies or autonomous bodies using public funds. If any private company is using public funds and/or functioning under the Government, then they will also be under the scrutiny of the NDSAP.

44 The Companies (Accounts) Rules also does not make a distinction between local and foreign companies, and takes into account all listed companies, and unlisted and private companies under certain specifications.

45 The M2M Roadmap has a sectoral approach that encompasses various industries, yet no specific mention has been made as to a distinction between local and foreign companies.

46 The only distinction made by the guidelines on cloud service providers is on the basis of the location and security of data – regardless of which country the service provider originates from, the data must be stored in India.

47 Localisation requirements in India mainly encompass data that are collected from local citizens in the midst of their use of applications, gateways or other related technology.⁵⁰

48 These requirements will apply to the private sector depending upon certain specifications, as are mentioned in the NDSAP and the Companies (Accounts) Rules. The law is unclear on whether operators in other sectors can store the data overseas by default, as there exists no specific legislation that delineates the data localisation requirements with respect to private and public sector, and demarcates the obligations of organisations across the board.

49 With regard to the telecom sector and data collected by government agencies such as Aadhar, data localisation is mandatorily done in order to preserve national security and the privacy of citizens.

50 See para 4.2.7(2) of the National Telecom M2M Roadmap at p 40.

50 With regard to the data collected by the citizens of India for the Aadhar initiative, the vast amount of information is stored in fully secured servers in its own data centre, located within the borders of India.⁵¹ UIDAI has issued statements guaranteeing that the data are protected, and that the outside world has no access to the data. This proves that the concept of data localisation *vis-à-vis* the Aadhaar Regulations has been enforced and implemented.

51 The National Security Council Secretariat (“NCSC”) looked to implement strong data localisation elements with regard to local e-mail servers and data being generated in India being brought under Indian laws, and these have also been enforced.⁵² For example, Blackberry servers allowed the Government the power to intercept messages and e-mails, as well as track browsing data.⁵³

52 The White Paper released by the Justice Srikrishna Committee delves into the issue of data localisation and recognises the need for carefully balancing the enforcement benefits of data localisation with the costs involved pursuant to such requirement. The paper eschews a one-size-fit-all model and suggests that different types of data will have to be treated differently.

D DEFAULT POSITION ON INTERNATIONAL DATA TRANSFERS, SCOPE AND TERRITORIAL EFFECT OF SECTION 43A OF IT ACT

i *Default position of section 43A IT Act and Rules*

53 As noted earlier, rule 7 of the Section 43A Rules provides that “sensitive personal data or information”, and not all categories of personal data, may be disclosed (whether within or outside India) only if that disclosure is necessary for the performance of the contract with the

51 <<https://timesofindia.indiatimes.com/business/india-business/aadhaar-data-kept-processed-only-on-own-secure-servers-uidai/articleshow/60342148.cms>> (accessed 26 March 2018).

52 <https://www.aicasia.org/wp-content/uploads/2017/06/OCC32014__1.pdf> (accessed 26 March 2018).

53 <<http://www.wired.co.uk/article/blackberry-india>> (accessed 26 March 2018).

provider of information, or where the provider has consented to the transfer.

54 Under current law, the default position is that of international transfers of sensitive personal data under section 43A of the IT Act authorised under conditions, with exceptions in case of the cumulative application of localisation requirements. For instance, under the telecommunications laws, all customer accounting and user information (other than roaming information) must be stored in India and cannot be transferred outside of India, and remote access to such data from outside India is prohibited in all cases.

ii *Scope of application of section 43A and rule 7*⁵⁴

55 Rule 7 of the Section 43A Rules sets conditions for the transfer of sensitive personal data outside India. It states:⁵⁵

A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer. [emphasis added]

a **Organisations covered**

56 A challenge that is apparent and must be dealt with under the rules is the lack of clarity with regard to rules for data controllers, processors and the differing scope of such rules. Indeed, section 43A of the IT Act and the 2011 Rules do not distinguish between controllers, processors or intermediaries, so the same set of laws apply to all parties given that they

54 For a critical analysis of the scope of s 43A of the Information and Technology Act, 2008 and the 2011 Rules, see Graham Greenleaf, *Asian Data Privacy Laws* (Oxford University Press, 2014) at p 414.

55 Information and Technology (Amendment) Act, 2008 s 43A (available at <<http://www.eprocurement.gov.in/news/Act2008.pdf>> (accessed 26 March 2018)).

are a “body corporate”. Without delineating the working of these notions, there may be situations where multiple rules apply to the same controller or processor – leading to confusion and hampering efficiency.

57 The notion of “body corporate” is defined by explanation (i) of section 43A as “any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities”. On 24 August 2011, a press note clarified that the 2011 Rules are applicable to “the body corporate or any person located within India”.⁵⁶

58 Transfer is only permitted if it is necessary for the performance of the contract with the data subject, or where the provider has consented to the transfer. The obligations relating to disclosure of personal data (whether within or outside India) will also apply to third-party processors.

59 Rule 7 applies to both domestic and international transfers, and to all parties, domestic and foreign. Therefore, distinctions in how foreign bodies are defined are not relevant for this purpose.

b Type of data covered by section 43A

60 Under the 2011 Rules, the data transfer rules only apply to “sensitive personal data or information” and do not apply to all personal data.

61 Sensitive personal data or information of a person means:

[S]uch personal information which consists of information relating to: (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail

56 Ministry of Communications & Information Technology, “Clarification on Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 under section 43A of the Information Technology Act, 2000 <http://meity.gov.in/writereaddata/files/PressNote_25811.pdf> (accessed 26 March 2018).

relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise. [rule 3]

62 In that definition, personal information means “any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person” (rule 2(1)(i)).

63 Biometric information is defined by reference to the concept of “biometrics” which means “the technologies that measure and analyse human body characteristics, such as ‘fingerprints’, ‘eye retinas and irises’, ‘voice patterns’, ‘facial patterns’, ‘hand measurements’ and ‘DNA’ for authentication” (rule 2(b)).

64 The notion of personal information refers to all natural persons, therefore, it does not distinguish between *data of residents and foreign individuals*. In this respect, it is interesting to note that the 2014 Bill extends the right to privacy to “all residents of India”. This is in contrast to the 2011 Bill, which extended the right to privacy to “citizens of India”. The 2014 Bill furthermore recognises the right to privacy as a part of Article 21 of the Indian Constitution and extends to the whole of India, whereas the 2011 Bill did not explicitly recognise the right to privacy as being a part of Article 21, and excluded Jammu and Kashmir from its purview.

65 “Public data” falls outside the scope of application of rule 7, which provides that “any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules”.

66 There are no laws which exclude “data in transit” from the scope of application of laws.

67 There are no clear regulations in Indian laws dealing with international transfer of anonymised, pseudonymised or encrypted data. However, the definition of personal data includes information through

which any individual may be directly or indirectly identifiable. Therefore, datasets which are de-identified using robust methods may fall outside the scope of personal data, and hence the data transfer laws may not be applicable to such datasets.

E LEGAL BASIS, MECHANISMS FOR DATA TRANSFERS, LIABILITY

68 Under rule 7 of 2011 Rules, the obtaining of consent is mandatory for data processing practices by body corporates of sensitive personal data or information. The regulation does not specify the form or nature of consent. There is no onshore data storage restriction implied by the consent obligations.

69 Rule 7 prescribes that data transfer abroad is allowed if:

- (a) the “same level of data protection” found under the 2011 Rules is ensured in the country of destination; and
- (b) only if it is “necessary for the performance of the lawful contract” between the body corporate or any person on its behalf and provider of information; or
- (c) where such person has “consented to data transfer”.

70 While there is an obligation on the data exporter to ascertain that the recipient is in a jurisdiction providing the *same level of data protection* as provided by the data exporter,⁵⁷ no process has been established for formally recognising that the jurisdiction meets these standards on par with India. Nor does the law list any substantive standards (*ie*, ratification of an international data privacy instrument, existence of a Data Protection Commission) to establish that the law of another jurisdiction establishes comparable data protection standards. *A fortiori*, there are no enabling provisions in Indian law under which a procedure for recognising sectoral adequacy can be established, neither is there any

57 Ministry of Communications & Information Technology, “Clarification on Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 under section 43A of the Information Technology Act, 2000 <http://meity.gov.in/writereaddata/files/PressNote_25811.pdf> (accessed 26 March 2018).

formal process to recognise jurisdictions with comparable or equivalent, or inadequate data protection standards. This is strongly recommended.

71 There is no additional guidance that has been provided on the interpretation of this abovementioned clause, for instance on where a data transfer is necessary for the performance of the lawful contract between the data controller and data subject.

72 There is no specific obligation on the data exporter to conclude a *contract with the data importer* under section 43A of the IT Act or the 2011 Rules. The only obligation, as stated above, is the need to ascertain that the recipient is providing the same level of data protection as provided by the data exporter or as required by the regulations. There is no restriction on transfer of data for the performance of a contract as long as the recipient is providing the same level of data protection as provided by the data exporter.

73 However, other jurisdictions such as the EU specify certain modes for transfer of data, and they are dependent on certain enumerated rules. For example, Indian companies may have to deal with regulations and standard contractual clauses if they are to collect and process data from customers in the EU, which works as one of the EU's ways of maintaining data protection and security with respect to dealings with third-world countries that do not share the adequate level of protection.

74 Accordingly it has become standard practice to use the approved European Commission model clauses wherever EU-based outsourcing involves data transfer and offshore processing in India. These clauses, which provide an alternative lawful means of data transfer, place strict obligations on both parties to ensure privacy of data and are considered by some to be onerous and to act as a disincentive for business.⁵⁸

75 Not being a member of APEC, India has not joined the APEC Cross-border Privacy Rules ("CBPR") System and the system cannot be used to demonstrate compliance with the requirements of rule 7.

58 Tim Wright, "India Demands EU Data Secure Nation Status But Still Lacks Robust Data Protection Laws" <www.sourcingfocus.com/site/opinionsitem/5308> (accessed 26 March 2018).

76 Presently it is not certain that certification mechanisms, privacy seals and trustmarks delivered abroad could be considered as a valid means for a data exporter to demonstrate that the “same level of data protection” in the country of destination as in India. However, it is interesting to note that the TRAI consultation paper on “Privacy, Security, and Ownership of the Data in the Telecom Sector”⁵⁹ raises questions about market incentives towards ensuring privacy – indicating the potential of certification mechanisms, privacy seals and trustmarks.

77 It has not been specified that certification or codes of conduct could play a similar role under rule 7. Today, rule 8(2) has recognised international Standard IS/ISO/IEC 27001 on “Information Technology – Security Techniques – Information Security Management System” as the only information security standard clearly recognised by the law governing processing and transfer of electronic data.

78 Further, rule 8(3) specifies that: “Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule (1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation”. It thus provides body corporates with the option of adhering to *codes of best practices* for data protection that have been developed by an industry association and approved and notified by the Central Government. Despite this option, sectors in India have not developed their own codes of best practices to fulfil this requirement. Yet, generally speaking, India appears to favour a self-regulatory/co-regulatory approach to privacy. Such an approach was recommended in the “Report of the Group of Experts on Privacy”⁶⁰ and reflected in the leaked 2014 Bill.⁶¹

59 <http://www.trai.gov.in/sites/default/files/Consultation_Paper%20on_Privacy_Security_ownership_of_data_09082017.pdf> (accessed 26 March 2018).

60 <http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf> (accessed 26 March 2018).

61 <<http://164.100.47.4/BillsTexts/RSBillTexts/asintroduced/data%20-E.pdf>> (accessed 26 March 2018).

79 Different government reports that deal with regulation of technology companies have endorsed the idea of a *regulatory sandbox*⁶² which would seek to lessen the regulatory burdens on small companies engaged in innovative practices. This suggests a growing belief that the needs of smaller companies in certain sectors need to be taken into account to allow them to flourish, however, these discussions are focused primarily on financial regulation, and not the data protection aspects of regulation which applies to these companies.

80 More specifically, Indian legislation does not cover the aspect of *interoperability*, but considering the multinational corporations that operate out of India and the culture of outsourcing that has financially benefited Indian companies – there appears to be sufficient demand from the IT industry in India for cross-border interoperability – particularly with the EU.

i *Liability*

81 The data exporter is liable in cases where the export of sensitive information and subsequent breach leads to wrongful loss or injury to the data subject if it is found that the exporter was negligent in implementing and maintaining reasonable security practices and procedures as defined under the Section 43A Rules.⁶³ Going by the White Paper released by the Justice Srikrishna Committee, it appears that obligations and corresponding liabilities should apply across both sensitive and non-sensitive personal data. Currently, there are limited provisions on liability in the existing data protection provisions, and it is expected that the data protection legislation will address these issues for both data exporters and data importers, keeping in mind the enforcement capacity of the regulator, both domestically and internationally.

62 See “Report of the Household Finance Committee” by the Reserve Bank of India, available at <https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=41471> (accessed 26 March 2018), and Report by “Watal Committee on digital payments” constituted by the Ministry of Finance, available at <http://finance.du.ac.in/du-finance/uploads/pdf/Reports/watal_report271216.pdf> (accessed 26 March 2018).

63 Information Technology Act, 2000 s 43A.

82 As of now, the factors that appear to weigh on the minds of companies in terms of liability have more to do with other regulations such as the GDPR. Considerations whilst deciding the instrument of data transfer are the efficiency of the instrument, the kind of penalty it may attract if data is leaked in any way, and the profitability of working with companies abroad.⁶⁴ Under the GDPR, Indian companies should not agree to standard contractual clauses that go against the strict regulations that the Foreign Exchange Management Act (“FEMA”) has with regard to foreign exchange as this may cause serious issues *vis-à-vis* the Reserve Bank of India (“RBI”), considering these clauses in question can lead to the depletion of large amounts of foreign exchange that companies must request the RBI for. For example, Tata Consultancy Services (“TCS”) was involved in a data breach incident that led to a fine of a US\$940m that was to be paid in foreign exchange.⁶⁵ Especially with the onset of the GDPR regulations that ask for 4% of the global turnover of the company as penalty, Indian companies will have to be more careful in the means of data transfer and processing.

F INTERNATIONAL CO-OPERATION ON DATA PROTECTION AND PRIVACY

83 It is unclear at this time whether there will be a dedicated privacy enforcement authority, or the different sectoral regulators will implement data protection laws in their specific domains. The White Paper released by the Justice Srikrishna Committee definitely seems to lean in favour of the creation of a data protection authority, which would be the appropriate authority to lead conversations on international co-operation on data protection. The provisional view in the White Paper is that a separate and independent data protection authority may be set up in India for enforcement of a data protection legal framework. The paper view is that there are three broad categories of functions, powers and

64 <<http://privacy.ind.in/wp/2017/04/30/under-gdpr-indian-data-processors-should-not-agree-to-standard-contractual-clauses-which-are-ultra-vires-the-fema/>> (accessed 26 March 2018).

65 <<https://economictimes.indiatimes.com/tech/ites/us-jury-slaps-940-million-fine-on-tcs-tata-america-international-corp-in-trade-secret-case/articleshow/51853894.cms>> (accessed 26 March 2018).

duties which may be performed by a data protection authority: monitoring, enforcement and investigation; standard-setting; and awareness generation.

Jurisdictional Report

THE REPUBLIC OF INDONESIA

Reporters: **Justisiari P Kusumah***

K&K Advocates

Danny Kobrata*

K&K Advocates

A GENERAL LEGAL FRAMEWORK OF INTERNATIONAL DATA TRANSFERS

i *Existing and pending data privacy protections in national legislation*

1 As there is no comprehensive Data Protection Act in Indonesia at present, there are no comprehensive rules on cross-border data transfers. Only a series of regulations provide for general personal data protection without detailed guidelines or specific processes attached. However, a comprehensive Data Protection Bill is due to replace the data protection provisions currently in force in Indonesian law in the near future.¹ The “Kementerian Komunikasi dan Informatika” (“Kominfo”), in English the “Minister of Communication and Informatics” or “MCI”, is responsible for the drafting of the Data Protection Bill, and other governmental institutions are currently being consulted to ensure harmonisation with sectoral regulations.

2 Under the current state of legislation, Article 26 of Law No 11 of 2008 concerning Electronic Information and Transactions (“Law 11/2008” or “EIT Law”) mandates that the “use of any information through electronic media that involves personal data of a Person must be made with the consent of the person concerned”. Law 11/2008 has been

* The reporters would like to thank Professor Sinta Dewi for her guidance and insightful input during the preparation of this report. All errors are these reporters’ own.

1 See Kharishar Kahfi, “Personal Data Protection Bill ‘Priority’ for House, Ministry Claims” *Jakarta Post* (8 November 2017).

amended by Law No 19 of 2016 (“Law 19/2016”), which has included in its Article 26 a right of individuals to request the deletion of his personal data, as well as to request the deletion of personal data where they are no longer relevant (the so-called Indonesian “right to be forgotten”).²

3 In addition, Article 15(1)(c) of Government Regulation No 82 of 2012 on the Implementation of the Electronic Transactions and Information Law (“GR 82/2012”³) requires that any electronic system provider (*ie*, “any Person, state agency, Business Entity, and community that provide, manage, and/or operate Electronic System individually or jointly to Electronic System User for its interest or other party’s interest” (Article 1(4)) must ensure that the collection, use and disclosure of personal data is based on consent from the “owner of personal data” (*ie*, the data subject), unless otherwise provided by regulations. Data may be disclosed to a third party only if that disclosure is in line with the original purpose for which the data had been originally collected from the data owner.

4 On 1 December 2016, MCI issued Regulation No 20 of 2016 concerning Personal Data Protection in Electronic Systems (“MCI 20/2016”) as an implementing measure mandated by GR 82/2012. This specific Regulation contains more detailed provisions on how to use personal data in electronic systems than Law 11/2008 and GR 82/2012. The Regulation provides a two-year transition period for full compliance of the law, *ie*, until 1 December 2018.

5 More specifically, Articles 21 and 22 of MCI 20/2016 govern cross-border data transfers:

- (a) Article 21(1) requires that any display, announcement, transfer, dissemination or provision of access to personal data in an electronic system can take place only with the individual’s consent unless otherwise regulated by other applicable laws and

2 See Andin Aditya Rahman, “Indonesia Enacts Personal Data Regulation” (2017) 145 *Privacy Laws & Business International Report* 1 at 6.

3 An unofficial bilingual translation of GR 82/2012 is available at <<http://www.bu.edu/bucflp-fig/files/2012/01/Law-No.-11-Concerning-Electronic-Information-and-Transactions.pdf>> (accessed 7 April 2018).

regulations, after the verification of the accuracy of the personal data and that it is in line with the purposes of gathering and collecting the personal data.

- (b) Article 22(1) mandates that any cross-border transfer of personal data outside of Indonesia is to be co-ordinated with MCI or an authorised entity, as well as comply with applicable laws and regulations on cross-border transfer of personal data.⁴ These provisions will be further elaborated on below.

6 Once passed, the new Data Protection Act of Indonesia is likely to change the applicable provisions on international transfers. Article 35 of the current draft Data Protection Bill⁵ provides that the transfer of data outside of the territory of the Republic of Indonesia is forbidden, unless:

- (a) the country of destination has an equal or greater level of protection as compared to the Data Protection Bill;
- (b) a contract has been concluded between the personal data controller and the third party outside of the territory of the Unitary State of the Republic of Indonesia; or
- (c) an international agreement has been concluded between the government of Indonesia and the government of the country where the data is to be transferred.

4 Article 22 of MCI Regulation 20/2016 concerning Personal Data Protection in Electronic Systems provides:

(1) Before transferring personal data overseas, an Electronic System Provider, whether a governmental institution, regional government or a company or private entity domiciled in the territory of Republic of Indonesia abroad, must:

- (a) coordinate with the MCI or authorized official/entity; and
- (b) implement the laws and regulations applicable to cross-border transfer of personal data.

(2) The requirement of coordination provided in Article 22(1) above can be satisfied in the forms of:

- (a) submitting of implementation plan of personal data transfer, which must at least contain the full name of target country, full name of recipient, date of transfer, and reasons/purposes of transfer;
- (b) requesting advocacy, if required; and
- (c) submitting the implementation report.

5 See the official version released for public consultation <<http://peraturan.go.id/rancangan-undang-undang-tentang-perlindungan-data-pribadi.html>> (Bahasa Indonesia only) (accessed 17 April 2018).

The data controller may be exempted from the obligations stipulated in Article 35 upon decree issued by the “Commission” (Article 42(4) of the current draft Data Protection Bill). The exemption may be granted following assessment by the Commission, to be issued in writing. The Commission may also revoke such exemption at any time.

7 Article 36 of the current draft Data Protection Bill further requires that any personal data controller who intends to transfer personal data to a third party abroad must first request and obtain written consent from the data subject. The consent requirement which is currently applicable under existing data protection regulations will therefore remain applicable.

8 Interestingly, the current version of the draft expressly provides that the regulation of personal data aims, among others, at “ensuring that the transfer of personal data is conducted in a limited manner” (Article 3(d)).

ii Constitutional protections

9 While the 1945 Constitution of the Republic of Indonesia (“Indonesian Constitution”) does not expressly mention the right to privacy, Article 28G of the Indonesian Constitution guarantees every person the right to protection of his/herself, family, honour, dignity and property, and the right to feel secure against and receive protection from the threat of fear to do or not do something that is a human right, and is considered to have impliedly conferred the protection of the right to privacy.

10 The Indonesian Constitutional Court has also decided in the *Constitutional Supreme Court Decision No 5/PUU-VIII/2010 dated 24 February 2011* that the scope of Article 28G of the Indonesian Constitution includes the right to privacy.⁶ The court found that the act of interception of communications was against the Indonesian Constitution on the grounds that it is against the right to privacy. Consequently, the court granted the request of the applicant to revoke

6 See <<http://hukum.unsrat.ac.id/mk/mk-5-puu-viii-2010.pdf>> (Bahasa Indonesia only) (accessed 7 April 2018).

Article 31 of Law 11/2008. It should be noted that Law 19 of 2016 as an amendment to Law 11/2008 has accommodated this decision of the court by amending the provisions of Article 31 accordingly.

11 By way of consequence, the Preamble to the draft Data Protection Bill that is soon to be introduced in Parliament also provides that “the protection of personal data is one of the forms of human rights that cannot be derogated from, as part of self-protection mandated by the Constitution of the Republic of Indonesia which entails the respect towards the value of human rights, equality and recognition of rights”, so that “the person should be provided with a firm legal basis in order to increase the protection of his/her personal data”.

iii *International commitments*

12 Indonesia has been a signatory to the International Covenant on Civil and Political Rights (“ICCPR”) since 1976 and ratified the ICCPR in 2006. In addition, Indonesia also signed the Optional Protocol to the ICCPR in 1976 and the Second Optional Protocol to the ICCPR in 1991.

13 Indonesia has not concluded any free trade agreements (“FTAs”) of its own regarding cross-border data transfer. However, the Association of Southeast Asian Nations (“ASEAN”) Economic Community (“AEC”) has concluded various FTAs with other Asian countries which contain data protection clauses. As an ASEAN Member State, Indonesia is bound by these clauses.

14 Although Indonesia joined the Asia-Pacific Economic Cooperation (“APEC”) in 1989, it has neither chosen to participate in the APEC Cross-border Privacy Enforcement Arrangement (“CPEA”), lodged a Notice of Intent to participate in the APEC Cross-Border Privacy Rules (“CBPR”) system, nor indicated any plan to join the system in the future.

15 As an ASEAN Member State, Indonesia is involved in the initiative on the development of a framework on digital data governance

under the Master Plan on ASEAN Connectivity 2025 (“MPAC”),⁷ which covers the issue of privacy protection measures and cross-border enforcement of personal data protection. The initiative is to be fully implemented by the end of the period 2018–2025. Indonesia is also a signatory to the ASEAN Human Rights Declaration adopted by ASEAN members at its 18 November 2012 meeting in Phnom Penh, Cambodia.

16 Indonesia is an observer on the Consultative Committee of the Council of Europe 108.⁸ It has not subjected an application to be recognised by the European Union (“EU”) as awarding an adequate level of personal data protection in the meaning of Article 25 of Directive 95/46/EC, and it is anticipated that the European General Data Protection Regulation (“GDPR”) will have minor impact on the data processing activities of businesses in Indonesia, as Indonesia is not a common destination for the outsourcing of personal data from the EU, and only a few companies store or otherwise process the personal data of EU residents.

iv Role of Minister of Communication and Informatics

17 Indonesia does not have any specific Privacy Enforcement Authority (“PEA”). Currently, MCI is the sole authority regulating the implementation of existing privacy regulations in Indonesia, administering Law 11/2008, GR 82/2012 and MCI 20/2016 discussed above. It is neither an Accredited Member nor an Observer of the International Conference of Data Protection and Privacy Commissioners. The role of MCI regarding cross-border data transfers is further detailed below.

7 See <<http://asean.org/storage/2016/09/Master-Plan-on-ASEAN-Connectivity-20251.pdf>> (accessed 7 April 2018).

8 Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe – “Observers – State of play and admission criteria”, T-PD(2018)04, 18 January 2018.

18 Under the Data Protection Bill, a Personal Data Protection Commission will be established with the authority to implement the law and settle personal data disputes out of court. Nevertheless, this is still subject to change, and there remains a possibility that MCI will remain as the enforcement authority.

v *Personal data transfers in financial sector*

19 The only current restriction on sectoral data transfers is in relation to financial service regulations. Article 31 of the Financial Services Authority Regulation Number 01/POJK 07/2013 Concerning Consumer Protection in Financial Sector stipulates that a financial service institution is not allowed to transfer consumer data and/or information to third parties, unless (a) the consumer has provided consent in writing, or (b) it is required by laws and regulations.

20 This restriction applies to both local and international data transfers. The Indonesian Financial Services Authority or “Otoritas Jasa Keuangan” (“OJK”) can impose sanctions in cases of non-compliance with the personal data rules.

B DEFAULT POSITION, SCOPE AND TERRITORIAL EFFECT

i *Default rule*

21 As a rule, transfers of personal data outside of Indonesia cannot take place unless conditions defined in the law are complied with. The same default rule will apply after the passing of the Data Protection Bill if its Article 35 is adopted in its current version, but with further specification on the conditions required to lift this ban.

ii *Extraterritorial scope*

22 The obligations in MCI 20/2016 to obtain the individual’s consent and to verify the accuracy of personal data before transferring the data apply to both local and foreign electronic system providers (“ESPs”). Indeed, the Regulation is an implementing measure of Law 11/2008, which expressly applies to Indonesian or foreign citizens, as well as

Indonesian or foreign legal entities whose actions outside Indonesia have legal implications in, or harms the interests of, Indonesia (Article 2 of Law 11/2008). The notion “harms the interest of” is referred to as interests “in connection with the national economy, strategic data protection and the dignity, protection, defence and sovereignty of the nation, citizens and legal entities” in the explanatory memorandum of Law 11/2008.

23 The obligation to co-ordinate with MCI under Article 22 of MCI 20/2016 applies to all ESPs (whether in the public or private sector), but only when they process data in relation to governmental institutions, citizens and/or private entities that are established in Indonesia.

iii *Type of organisations covered*

24 Today, no distinction is made between “controllers” and “processors” under the law, which only refers to “ESP”. No exemptions are made for specific categories of sectors or companies, and the amount of personal data processed by an ESP is not a consideration in the provision of exemptions. As mentioned above, the notion of an ESP, as defined by the EIT Law and its implementing Regulations, is very broad and covers, in practice, any organisation in the public or private sector that operates an electronic system to manage personal data, whether for internal or external purposes (*ie*, management of employee or customer/client data).

25 The current version of the Data Protection Bill, on the contrary, distinguishes between “Personal Data Controllers” and “Personal Data Processors”, the latter being “organisations conducting personal data processing on behalf of personal data controllers” (Article 1(4)).

iv *Type of data covered*

26 Personal data is very broadly defined by GR 82/2012 and MCI 20/2016 as “certain individual data relating to an individual, whose accuracy, confidentiality, and protection must be ensured”. Article 1(2) of MCI 20/2016 further specifies that the definition of certain individual data must be understood as information which is true and valid, and

which is inherent to the individual who can be identified, whether directly or indirectly, through this information.

27 Data export requirements apply to all personal data with no distinction between “specific data” or “non-specific data”. However, it should be noted that under Article 6 of the draft Bill, a provision relating to “specific personal data” includes information on religion/belief, health, biometric, genetics, sexual life, political preference, criminal record, children data, personal financial data, and other data according to applicable laws and regulations. The categories of data referred to under Article 6 are similar to the categories of data commonly included in the definition of “sensitive data” under European law.

28 Any data collected and processed in Indonesia falls under the law, regardless of the nationality of the personal data owner and whether they are “data in transit”. The current version of the Data Protection Bill explicitly mentions that persons covered by the Act are “citizens”, “whether Indonesian citizens or foreign citizens in Indonesia”. However, this definition is vague as to whether this refers to the data subjects or the data controllers and processors. Any consideration as to whether data falls under the law should hence be considered in the context of its territorial scope, which appears to focus more on the impact to Indonesia’s interests.

29 The law is silent regarding the issues of anonymisation, pseudonymisation and data encryption, except MCI Regulation 20/2016 which requires all ESPs to store personal data in encrypted form. Under the law, one of the requirements for data to be considered as personal data and protected by the law is that the data are attached and identifiable, either directly or indirectly, to an individual. If anonymisation, pseudonymisation or data encryption causes the data to be unidentifiable to an individual, then the data may fall beyond the application of the law. MCI has not published any available guidance on the interpretation and utility of anonymisation, pseudonymisation and data encryption.

C LEGAL BASIS

i *Data subject's consent*

30 As mentioned earlier, unless otherwise provided by regulations, the individual's consent is always required for the transfer of personal data. No alternative legal basis (*eg*, transfer necessary for the performance of a contract between the data owner and the ESP) applies. No provision explicitly requires consent to be given in the form of an express opt-in. However, in practice, the ESP needs to obtain an express opt-in from the data subject to transfer the data since Article 6 in conjunction with Article 1(4) of MCI 20/2016 provides that consent must be obtained in writing (manually and/or electronically) after the personal data owner has received full explanation regarding the acts of processing, collecting, obtaining, analysing, storing, displaying, announcing, transferring and disseminating as well as confidentiality and non-confidentiality of the personal data. Furthermore, such consent can only be given after the owner has confirmed the accuracy and confidentiality of the data.

31 It should be noted that the form through which the data subject's consent is obtained should be drafted in Bahasa Indonesia. However, it may be drafted in another language, provided the version in the original language is available.

32 Article 8 of the draft Bill requires the data controller to obtain the individual's consent to collect and process specific personal data relating to him or her. Furthermore, Article 9 of the draft Bill expressly stipulates that this consent must be provided in writing.

ii *Co-ordination with MCI*

33 Any transfer of personal data outside Indonesia requires co-ordination with MCI, which must be conducted through the methods stipulated under Article 22 of MCI 20/2016, namely:

- (a) submitting an implementation plan of personal data transfer to MCI and notifying MCI about the plan to transfer personal data outside of Indonesia;
- (b) "advocacy", if applicable, *ie*, requesting an advice in the form of consultation with MCI; and

- (c) submitting an implementation report to MCI by filing a report regarding the transfer to MCI within a certain time after the transfer has been completed.

34 The term “advocacy” refers to the procedure provided by MCI to facilitate/mediate a discussion between a data subject and the transferring party if any misconduct were to happen. The advocacy serves as a medium to facilitate an amicable settlement between the two parties. At present, there has not been any precedence of a data subject exercising the right of advocacy.

35 While the purpose of this procedure is not made explicit in the law, it is understood that the purpose of conducting “co-ordination” with MCI before transferring personal data outside Indonesia is to allow the Government to monitor the outward flow of information. The co-ordination takes place by submitting an implementation plan letter with other supporting documents (*eg*, power of attorney if submission is made by attorney) to the Directorate General of Application and Informatics of MCI. After the transfer of data is completed, the exporting company will have to submit an implementation report to the MCI within a certain period.

36 As several of these ambiguous provisions have proven to be difficult to implement in practice (*eg*, how often reports should be made if data are transferred on a regular basis), MCI seems to have agreed to issue further clarifications on some of them.

37 The law remains silent on whether MCI can refuse a transfer of personal data outside Indonesia. The “co-ordination” requirement set out under the law seems closer to a notification requirement than to an application for approval. However, by experience, the Indonesian government may send a letter requesting the transferring organisation to cease the transfer of personal data if it objects to a transfer of personal data. The law does not specify whether an appeal can be filed against such a *de facto* prohibition of transfer of personal data by the Government. However, it would be possible to file a civil or administrative claim against the Government in such situations.

38 The current draft Data Protection Bill is silent regarding the co-ordination obligation after the enactment of the Personal Data Protection Bill. However, Article 57 of the current draft Data Protection Bill provides that all existing laws and regulations in relation to the processing of personal data shall remain applicable to the extent that they *do not contradict* the Personal Data Protection Bill.

39 As the co-ordination obligation stipulated in MCI 20/2016 is not contradictory to the Personal Data Protection Bill, it is likely that it will continue to apply after the enactment of the Personal Data Protection Bill. However, as the draft is currently in the process of being harmonised with other laws, revision to the draft Data Protection Bill (including the provision regarding the co-ordination obligation) must be anticipated.

D DATA LOCALISATION

40 Several data localisation regulations apply in Indonesia. The main ones concern ESPs offering public services and in the financial sector.

i *Electronic system providers offering public services*

41 GR 82/2012 and MCI 20/2012 require that all organisations providing a “public service” to locate their data centres and data recovery centres in Indonesia for data protection and law enforcement purposes. However, the data localisation requirements do not prohibit ESPs of public service (to which the localisation requirements apply) from transferring the data abroad as long as the ESP also stores a copy of the personal data in Indonesia.

42 Law No 25 of 2009 concerning Public Service (“Law 25/2009”) broadly defines “public service” as an activity or series of activities conducted to fulfil the need for service, in accordance with laws and regulations, for every Indonesian citizen, in relation to goods, services, and/or administrative services provided by public service operators. Law 25/2009 further defines a “public service operator” as any state administrator institution, corporation, independent institution which has

been established by law for the performance of a public service activity, and any other legal entity that is solely formed for public service activity.

43 Article 4(1) of Minister of Communication and Informatics Regulation No 36 of 2014 concerning Electronic System Provider Registration Procedure (“MCI 36/2014”) gives more details on the scope of the concept of a “public service operator”:

- (a) a state administrator institution which consists of state institution and/or government institution and/or relevant Work Unit Operator;⁹
- (b) a corporation in the form of a state-owned company (“BUMN”) and or regional state-owned company (“BUMD”) and/or relevant Work Unit Operator;
- (c) an independent institution established by law and/or relevant Work Unit Operator; or
- (d) any other legal entity which fulfils a mission of public service within the framework of implementation of State Missions.

44 Provisions related to State Missions are stipulated in GR 96/2012. These include services which should be carried out by the Government, but which, due to the limitation of government capability, are outsourced to a private entity which are funded by the Government by way of subsidies (*eg*, companies in transportation, healthcare and telecommunication). The current notion of “public service” has often been criticised as interpreted too widely, as it extends to the provision of services by non-government companies in areas as diverse as in banking and payment system, insurance, health, transportation, telecommunication, and education. Private companies operating in these sectors, therefore, must have data centres in Indonesia. Because of these criticisms, MCI announced in January 2016 that data localisation requirements would be eased, and an amendment is being prepared by MCI in that regard. As noted from various discussions involving MCI, the amendment might limit the applicability of the obligation to establish data centres and disaster recovery centres in Indonesia to only certain categories of data. However, following a recent discussion with the competent department

9 A Work Unit Operator (“Satuan Kerja Penyelenggara di lingkungannya”) refers to units or divisions within a state institution which have their own/special authority.

in the ministry, at this stage, there is no certainty about the outcome of this amendment, so caution must be observed. The draft is currently at the stage of internal harmonisation. MCI will release the draft for public consultation once the harmonisation process has completed.

45 Article 17(2) of MCI 20/2016 defines the data centre (for personal data processing) as a facility that is used to locate the electronic system and its related components for the purpose of locating, storing and processing data. This implies that the personal data must be kept in a physical facility in Indonesia but again the organisation may transfer the personal data outside Indonesia as long as it retains a copy of the data in Indonesia. Article 22(1)(b) of the regulation also provides that the transfer must comply with cross-border personal data exchange legislation, which will have full meaning when the Data Protection Bill is effectively passed.

46 Both GR 82/2012 and MCI 20/2016 must be consistent with Law 11/2008, of which they are implementing regulations. While GR 82/2012 and MCI 20/2016 remain silent on their territorial scope of application, Law 11/2008 provides that it (including its implementing regulations such as GR 82/2012 and MCI 20/2016) applies to those who reside in and outside Indonesian jurisdiction. For those residing outside Indonesia, Law 11/2008 applies only to the extent that the act of the persons (a) has legal implication within Indonesian jurisdiction and/or (b) has legal implication outside Indonesian jurisdiction but harms the national interest.¹⁰ National interest could mean economic interest, protection of strategic data, dignity, defence and security, sovereignty, and the interests of Indonesian citizens and legal entities.

47 This provision has already been used to request a major foreign company to establish its data centre in Indonesia. In addition, the Government has also issued implementing regulations which allow the

10 Article 2 of Law No 11 of 2008 concerning Electronic Information and Transactions provides:

This Law shall apply to any Person who commits legal acts as governed by this Law, both within jurisdiction of Indonesia and outside jurisdiction of Indonesia, having legal effect within jurisdiction of Indonesia and/or outside jurisdiction of Indonesia and detrimental to the interest of Indonesia.

Government to block access to a website which contains “negative” content. Such access to national and foreign websites has been blocked by the Government on several occasions.

48 Based on this provision, it appears that the data localisation requirement can apply to foreign entities if the processing or storing of personal data by the foreign entity is considered to have legal implication within Indonesian jurisdiction and/or to have legal implications outside Indonesian jurisdiction but harms the national interest. Observers mention, in any case, that as the Government is encouraging foreign businesses to establish a presence as a permanent establishment or by incorporating an Indonesian legal entity, this would have the effect of rendering data localisation requirements applicable in practice.¹¹

49 Furthermore, the law is silent on the exemption from data localisation requirements. While existing legislation does not grant the Government any legal ground to grant exemption of the data localisation requirement, based on professional experience, MCI may grant an exception after particular considerations.

50 Data localisation provisions came into force on 12 October 2012 upon the enactment of GR 82/2012. However, GR 82/2012 provides for a five-year grace period for compliance. The Government has been asking all ESPs to comply with this regulation over the past years, even though the regulation did not come into effect until 12 October 2017.

51 The position of the Government on this matter remains a little unclear, as the Minister of Communication and Information has stated that they are currently reviewing the policy, but also that they will enforce this obligation because the regulation is already in place.¹²

11 Aston Goad & Karina Antonio, “Data Localisation: Coming to You Soon in Indonesia” *Asian Legal Business* (November 2017) at p 33.

12 See <<https://pemeriksaanpajak.com/2016/12/14/wajib-punya-pusat-data-di-indonesia/>> (Bahasa Indonesia only) (accessed 7 April 2018).

ii *Data localisation in the financial sector*

52 As previously mentioned, all ESPs in the financial sector are required to store transaction data in Indonesia, regardless of whether they effectively fulfil a public service or not. “Transaction data” refers to data resulting from an “electronic transaction”. GR 82/2012 defines “electronic transaction” as any action with legal consequences made by using a computer, computer network and/or other electronic media.

53 Furthermore, it must be noted that already a few years back, MCI and OJK have announced plans to enact regulations requiring all foreign systems and transaction providers, especially foreign banks, to establish their own data centres in Indonesia.¹³

54 At present, the regulation POJK 38/2016 issued by OJK, which only applies to banks, requires them to locate their electronic system in data centres and disaster recovery centres in Indonesia.¹⁴

55 Under Article 50 of POJK 69/2016, insurance, Syariah insurance, reinsurance and Syariah reinsurance companies are also required to localise their data in data centres and disaster recovery centres located in Indonesia for law enforcement, protection and the recognition of state sovereignty. The regulation provides that at least the following data must be located in Indonesia:

- (a) data and information relating to the personal data of the policyholder, the insured or the participant;
- (b) data and information relating to premium payment transactions or claims;
- (c) population data and information; and
- (d) data and information in the administrative field of the legal entity.

13 See press release by Kominfo, 21 April 2015 <https://kominfo.go.id/index.php/content/detail/4791/OJK+Dorong+Pembentukan+Pusat+Data+Bank+Asing/0/sorotan_media> (available in Bahasa only) (accessed 7 April 2018).

14 Peraturan Otoritas Jasa Keuangan tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi Oleh Bank Umum.

56 POJK 38/2016, by contrast, does not contain any specific provision on the categories of data that must be localised in Indonesia.

57 There are exceptions to the localisation rule, however, where banks can host specific information outside of Indonesia with OJK's approval, provided that the data does not contain identifiable customer information. OJK has been reported as increasingly issuing helpful and practical guidance on these issues.¹⁵

E DATA TRANSFER MECHANISMS

i *Preliminary issues*

58 From a business viewpoint, having multiple systems of cross-border data transfer in Asia poses challenges to cross-border trade between Asian countries, as companies might have to comply with multiple systems of cross-border data transfer. This hinders the efficiency of data transfers within Asia and increases the cost of compliance with little benefit in sight.

59 Unlike the EU which has adopted Standard Contractual Clauses ("SCC") and Binding Corporate Rules ("BCR"), Indonesian law does not provide any mechanisms for the transfer of personal data besides consent. Further, there does not appear to have been any public demand made by companies in relation to interoperable personal data transfer instruments with other countries, and the Government has not yet taken any public stance on this issue.

60 While the law does not contain any specific provision compelling the exporter to ensure that the recipient established in a third country is legally bound to protect personal data, the extraterritorial scope of the law may apply to both the exporter and recipient. The law is silent on the liability of the local data exporter in the event of a breach by the data

15 See "Indonesia: Cloud in Financial Service", Regulatory Overview by Microsoft <<https://www.microsoft.com/en-sg/apac/trustedcloud/indonesia-financial-service.aspx>> (accessed 7 April 2018).

importer overseas, but in principle such liability will always be attached to an ESP who holds the data. This allows an importer to be held liable.

61 Consultation with an MCI official has led these reporters to understand that the exporter would be considered as liable, even in the event that the data have been transferred to another party, and regardless of the type of transfer mechanism used, in the case of a personal data breach abroad. The reason for this is that the data exporter is the party who originally collected the personal data directly from the personal data owner and bears the primary responsibility for ensuring the ongoing protection of the data transferred.

ii *“Adequacy findings” and white lists*

62 Today, the law does not require a foreign country to which personal data is transferred to have an adequate level of protection of personal data in relation to Indonesian law. However, the Data Protection Bill provides otherwise by stipulating that transfers could be free towards a country of destination which has an equal level of protection with the Data Protection Bill. However, the draft Bill does not specify which authority would make the assessment of the level of protection, nor which criteria would be used to carry out that assessment.

iii *Consent as exception to existence of privacy safeguards overseas*

63 Apart from the “coordination” requirement which MCI provided in Article 22 of MCI 20/2016, and unless otherwise provided by regulations, only the consent of the individual could permit transfer to a country without an adequate level of personal data protection. No guidance on the matter has been issued by the Government.

64 There do not appear to be any complaints from companies regarding the consent requirement. This is particularly so as the consent requirement, as it stands, does not prove to be onerous in practice. Companies only need to ensure that they have covered all transfer purposes in the consent form at the time of collection. In addition, the current cross-border transfer rules are relatively lenient compared to

other countries that have already enacted a developed personal data protection act.

iv *Contracts*

65 The data exporter and importer are not required to conclude a contract for the purposes of transferring personal data, nor is any similar guarantee required by the law. However, the joint adoption of standard clauses by several Asian countries could be useful to categories of companies such as small and medium-sized enterprises if it could exempt data exporters from regulatory obligations such as obtaining the user's consent and/or obtaining governmental authorisation for data transfers. Such standard clauses could have the added benefit of forcing the contractual parties (data importer/data exporter) to negotiate certain topics (*eg*, security, data retention and exit scenarios) and contractually allocate liability for these matters.

66 The different sets of European SCCs are rarely implemented in the jurisdiction, and even when implemented it is only to satisfy EU legal requirements in situations where data are temporarily transferred to the EU for storage or further processing.

v *Certification, trustmarks and privacy seals*

67 Certification of privacy management practices is not mandatory under the law, so companies remain free to choose if they want their privacy management practice to be certified by an agent. However, Article 28(a) of MCI 20/2016 requires the electronic system that is used for personal data processing to be certified. This obligation will apply once the Government issues the implementing regulation regarding the certification of electronic systems for personal data processing. As the implementing regulation has not been issued, it is not yet known whether the Government would take into account the impact to micro, small and medium-sized enterprises. Similarly, no other data transfer instruments can be implemented without any implementing regulation.

F INTERNATIONAL CO-OPERATION BETWEEN MCI AND FOREIGN PRIVACY ENFORCEMENT AUTHORITIES

i *Co-operation with foreign privacy enforcement authorities in areas other than enforcement*

68 No provision in the current legislation prevents MCI from developing operational co-operation with other PEAs. In addition, Article 39 of the current draft Data Protection Bill, in a Chapter entitled “International Cooperation”, requires the Government to take necessary measures to prevent personal data violations so as to improve international standards of personal data protection (paragraph 1), and to adopt a policy so that the rights of the personal data owners are not breached due to the transfer of data across borders (paragraph 2). However, to date, MCI has not concluded any bilateral or multilateral arrangements with the authorities of other jurisdictions to co-operate in the implementation of privacy laws.

69 MCI is also not bound by any obligation to ensure regional or international consistency in its decision-making process. However, the law mandates an academic paper to serve as the basis of drafting any new regulation. This academic paper will refer to the regional or international obligations that Indonesia has to comply with. Since the implementing regulation of any law must be consistent with the law itself, the implementing law will be consistent with regional or international treaties if the law has been drafted to be so.

ii *Enforcement of cross-border transfer restrictions in Indonesian law*

70 The enforcement of administrative sanctions for breach of provisions on the protection of personal data is currently handled within the authority of MCI. Criminal sanctions, on the other hand, are enforced by the police or a civil servant investigator from MCI. Law 11/2008 expressly allows the police or any other authorised criminal investigators to co-operate with foreign enforcement authorities by sharing the information and evidence in criminal investigations.

71 MCI may impose administrative sanctions if the transfer or dissemination of personal data is done unlawfully and in contravention of

applicable legal provisions. Administrative sanctions can take the form of verbal warning, written warning, temporary suspension of business and/or publication online. Under 53 of the current draft Data Protection Bill, the Commission shall be authorised to impose administrative sanctions against business actors for breach of the Act, such as orders to suspend the processing, to remove or delete the data, compensation payments, and/or imposition of fines.

72 The recent development of enforcement against cybercrime in Indonesia shows that the transfer of electronic information (which may include personal data) to an unlawful party may be subject to the criminal law with maximum eight years imprisonment and/or maximum fine of Rp2,000,000,000. This was brought about by recent enforcement of the law on cybercrime by the Indonesian National Police (“INP”). In particular, the INP have interpreted a provision on unlawful transfer of electronic information to include the unlawful/unauthorised transfer of data without consent of the data subject.

73 In addition, in a recent criminal case on trading of personal data handled by the police,¹⁶ the INP used its enforcement powers under criminal law upon the finding that the data transfer constitutes a criminal act.¹⁷ This pertains to a provision in Law 11/2008 which prohibits the unlawful transfer of electronic information and/or electronic documents to an unauthorised party. The definition of electronic information¹⁸

16 The Criminal Investigation Department (Bareskrim) arrested a suspect who was allegedly involved in an organised criminal operation selling the data of bank customers on 12 August 2017. Police revealed that the *modus operandi* was to collect customer data from banks’ marketing divisions or other marketing partners and sell the customer data through various websites and social media. The arrest was made as the Indonesian National Police were of the view that an unauthorised data transfer had occurred. See <<https://news.detik.com/berita/3610769/bareskrim-tangkap-jaringan-penjualan-data-nasabah-bank>> (available in Bahasa only) (accessed 7 April 2018).

17 See <<http://www.republika.co.id/berita/ekonomi/keuangan/17/08/25/ov8i59382-ojk-cermat-isi-formulir-bank-cegah-jual-beli-data-pribadi>> (available in Bahasa only) (accessed 7 April 2018).

18 Article 1(1) of Law No 11 of 2008 concerning Electronic Information and Transactions provides:

Electronic Information is one or a set of electronic data, including but not limited to text, sounds, images, maps, drafts, photographs, electronic data
(continued on the next page)

and/or electronic document¹⁹ is broad enough to cover personal data that are stored electronically.

74 In addition, the data subject may always claim compensation in a civil lawsuit, for instance under Article 26 of the EIT Law.

75 Article 26 of the EIT Law provides that MCI may receive complaints from personal data owners for the breach of personal data. Upon receiving the complete application of the complainant, MCI must hear and settle such complaint. The complaint can be settled amicably or via alternative dispute settlements. MCI may impose administrative sanctions regardless of whether the parties have settled amicably or solved the complaint via alternative dispute settlements.

76 For administrative sanctions, MCI will conduct an assessment and impose the sanctions. Currently, MCI has not established any policy regarding the assessment and sanction for breach of the cross-border transfer provision. For criminal sanctions, standard criminal procedure will apply to the assessment of the breach and the imposition of sanctions. MCI does not appear to have taken any action with regard to the transfer of personal data outside Indonesia.

iii *International enforcement by privacy enforcement authorities*

77 Currently, Indonesia is not party to any international or regional networks that adopt guidance or develop enforcement actions jointly, so

interchange (EDI), electronic mails, telegrams, telex, telecopy or the like, letters, signs, figures, Access Codes, symbols or perforations that have been processed for meaning or understandable to persons qualified to understand them.

19 Article 1(4) of Law No 11 of 2008 concerning Electronic Information and Transactions provides:

Electronic Document is any Electronic Information that is created, forwarded, sent, received, or stored in analogical, digital, electromagnetic, optical form, or similar form, which are visible, displayable and/or audible via Computers or Electronic Systems, including but not limited to writings, sounds, images, maps, drafts, photographs or equivalent, letters, signs, figures, access codes, symbols or perforations having certain meaning or definition or understandable to persons qualified to understand them.

that MCI does not participate in international networks such as the Global Privacy Enforcement Network (“GPEN”), APEC Cross-border Privacy Enforcement Arrangement (“CPEA”), International Conference of Data Protection and Privacy Commissioners Enforcement Cooperation Arrangement, or Unsolicited Communications Enforcement Network (“UCENet”).

78 The law does not provide for the transfer of complaints to authorities in other jurisdictions, and MCI has no bilateral arrangements with the authorities of other countries to co-operate in the enforcement of privacy laws.

79 MCI has not published any enforcement policy on data transfers or data localisation requirements. It has not been involved in co-ordinated efforts involving authorities from multiple countries over the past years. However, no general prohibition weighs on MCI to provide information to other enforcement authorities.

80 There do not appear to have been any joint investigations or co-operation on personal data breaches undertaken with foreign authorities, nor have there been any joint findings against a foreign controller based in multiple jurisdictions. However, cross-departmental investigation on data matters has already taken place within Indonesia, *eg*, in a recent case on the illegal sale of a bank customer’s data, which was handled by the police department with the support of the financial authority.²⁰

20 The Criminal Investigation Department (Bareskrim) arrested a suspect who was allegedly involved in an organised criminal operation that selling the data of bank customers. Police revealed that the modus operandi was to collect customer data from banks’ marketing divisions or other marketing partners and sell the customer data through various websites and social media. In relation to this case, the National Bank Association is working with the regulator, the Financial Services Authority (“OJK”) to find sources of customer data leakage. In addition, OJK also appealed to the public to always be vigilant and careful in providing personal data to anyone, including to the bank. See <<https://news.detik.com/berita/3610769/bareskrim-tangkap-jaringan-penjualan-data-nasabah-bank>> (available in Bahasa only) (accessed 7 April 2018).

Jurisdictional Report

JAPAN

Reporter:

Kaori Ishii*

Associate Professor, Faculty of Library, Information and Media Science, University of Tsukuba

Supporting expert:

Fumio Shimpo*

Professor, Faculty of Policy Management and Graduate School of Media and Governance, Keio University

A INTRODUCTION

1 Pursuant to Article 7¹ of the Act on the Protection of Personal Information (“APPI”), the Personal Information Protection Commission, Government of Japan (“PPC”) adopted the Basic Policy on the Protection of Personal Information (“Basic Policy”) on 14 October 2016, which was subsequently approved by the Cabinet on 28 October 2016.

2 Under the Basic Policy, the PPC strives to establish and maintain an environment for a smooth flow of data while ensuring the protection of personal information by participating in an international co-operative framework and building co-operative relations with foreign enforcement authorities.

3 The globalisation of economic and social activities and the development of information and communication technologies has led to an increase in cross-border data transfers, including personal information. Article 24 of the APPI was established to address the increasing need for

* The reporters would like to thank the Personal Information Protection Commission of Japan for providing useful advice.

1 Article 7 of the Act on the Protection of Personal Information provides: “The government shall establish a basic policy on the protection of personal information (basic policy) in order to seek to comprehensively and integrally promote measures concerning the protection of personal information.”

fixed rules regarding the transfer of personal data to foreign countries and for the purpose of harmonising with international frameworks regarding personal data protection, while respecting the basic principles of securing free flow of information in the Organisation for Economic Co-operation and Development “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” (“OECD Privacy Guidelines”).

4 The enactment of this policy was also requested by industry players who sought economic benefits from the free flow of personal data while having clear rules to ensure the appropriate protection of personal data in each jurisdiction.

5 A key driver of cross-border data transfers in the jurisdiction is technology such as broadband networks, smartphones, cloud computing and artificial intelligence that can effectively and efficiently collect, use and share massive amounts of data. The Japanese government recognises that the free flow of information is a fundamental principle promoting a global economy and innovation. An example of government action taken to address the issue is the G7 Principles and Actions on Cyber adopted on 27 May 2016.

6 Coupled with business conducted at both a regional and international level, such technology creates a greater push for cross-border data transfers. The Asian region is not only a principal market for industry development for the next generation in Japan, but it is also an important provider of cloud computing services, business process outsourcing, offshore developments, *etc.* Rules governing such cross-border data transfers are thus increasingly important to facilitate such transfers in the region while affording protection to the personal data of individuals.

7 Japan is not currently recognised by the European Union (“EU”) as providing an adequate level of protection for cross-border data transfers from the EU to Japan. Therefore, data transfers from the EU to Japan must follow the Standard Contractual Clauses or the Binding Corporate Rules, so far. However, a co-operative dialogue between Japan and the EU is underway to build a mutual personal data transfer framework. The PPC and the EU are accelerating work towards achieving mutual

adequacy findings in 2018, based on the constructive meeting on 14 December 2017 as stated below.

8 Similar frameworks include the EU-US Privacy Shield, while Korea has been trying to obtain recognition that its protections are adequate. To maintain the business competitiveness in Japan, a system to facilitate the ease of data transfer is critical. In line with this, Japan has also been part of the Cross-Border Privacy Rules System as of 2014, with certification having commenced in 2016.²

9 Japanese businesses have a culture of strict compliance with the law. As a result, business entities tend to err on the side of caution in relation to the processing of personal data out of fear of violating the APPI or infringing on privacy rights, resulting in restricted data flow in the business sector. Clearer rules relating to such transfers would thus encourage data flows without compromising on the protection of personal data.

10 However, differing provisions on cross-border data transfers, the definition of personal information and the conditions for consent in different countries results in unnecessary burdens on business entities to ensure legal compliance. Differing definitions of personal data causes discrepancies in protection when data may be considered “personal information” in one country but not in another. Furthermore, the differing conditions for consent (for instance, explicit or implied, opt-in or opt-out, *ex ante* or *ex post*) compels business entities to implement different procedures to ensure compliance.

11 According to a Ministry of Economy, Trade and Industry survey,³ from 1995 to 2014, the export value from Japan to the EU fell by 0.57–0.64% due to the legal regulations in EU Member States based on Directive 95/46/EC, while the import value from the EU to Japan fell by 1.03–1.35%. The negative impact of legal regulations is greater on the import value than on the export value.

2 Ministry of Economy, Trade and Industry, “Japan’s First Certification of a Business under the APEC CBPR System” (News Release, December 2016).

3 See <http://www.meti.go.jp/medi_lib/report/2016fy/000504.pdf> (in Japanese) (accessed 10 April 2018).

12 Article 24 of the APPI incorporates a provision restricting the disclosure of personal data to a third party in a foreign country. As the amended Act went into effect on 30 May 2017, there is no quantitative data and the impact of this provision on internal and external business entities remains to be seen.

B GENERAL LEGAL FRAMEWORK OF INTERNATIONAL DATA TRANSFERS

i *Existing data privacy protections in the national legislation*

13 The APPI is Japan's main data protection Act. Article 24 of the APPI governs cross-border data transfers out of Japan. It prescribes that the data subject must in principle have consented to the transfer of his/her information to a third party in a third country prior to any such transfer. Other national legislation concerning personal information include the Act on the Protection of Personal Information Held by Administrative Organs and the Act for the Protection of Personal Information Retained by Independent Administrative Institutions.

14 In addition, the Unfair Competition Prevention Act restricts the breach of trade secrets. Trade secrets often include consumer lists, which can be unlawfully disclosed by current or former employees. The Act was amended in 2015 to impose criminal sanctions on perpetrators having used or disclosed trade secrets outside Japan.

15 While Japan's Constitution does not explicitly address the protection of personal data or privacy, a constitutional right to privacy is granted in the second paragraph of Article 13, which provides that all people shall be respected as individuals, with their right to life, liberty and the pursuit of happiness being the supreme consideration in legislation and in other governmental affairs.⁴ This interpretation is well

4 Article 13 of the Constitution of Japan provides: "All of the people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental affairs."

established and non-controversial among scholars, lawyers and other stakeholders.⁵

16 Supreme Court decisions have acknowledged the legal interest of privacy. In the Supreme Court decision of 12 September 2003 (the *Lecture by Jiang Zemin at Waseda University* case),⁶ the Supreme Court ruled that providing private information to the police department without consent breaches the reasonable expectation for the appropriate management of such data, even if such provision of data was for security purposes. In this case, the University had invited Mr Jiang Zemin, the former President of China, to lecture in front of a large audience. It provided a list of the 1,400 students who attended the lecture to the Tokyo Metropolitan Police Department for security purposes but had not obtained the consent of the participants for such disclosure. In a previous case handed down by the Supreme Court on 14 September 2002,⁷ the plaintiff was granted an injunction and damages on account of the violation of her personality rights, including reputation and privacy, through the publication of a novel. In both rulings, the Supreme Court explicitly used the term “privacy”.

17 More recently, in a decision on 31 January 2017,⁸ the Supreme Court has also dealt with a dispute on the deletion of search engine results related to the plaintiff's criminal history of child prostitution. While this dispute is related to the “right to be forgotten” in the European Court of Justice decision on 13 May 2014⁹ and in the EU's General Data Protection Regulation (“GDPR”), the Supreme Court mentioned nothing about the “right to be forgotten” in its own decision.

5 Numerous scholarly papers on privacy and personal data protection in the field of constitutional law have already been published. One of the highly respected books recently published is Emeritus Professor Koji Sato (Kyoto University), *Theories on Japanese Constitution* (Seibundoh publishing, 2011), in which the right to privacy is clearly protected in the second paragraph of Art 13.

6 2002 (Ju) 1656 *Minsbu* No 57-8 at p 973.

7 2001 (O) 851 <http://www.courts.go.jp/app/files/hanrei_jp/093/076093_hanrei.pdf> (in Japanese) (accessed 1 February 2018).

8 2016 (Kyo) 45 *Minsbu* No 71-1.

9 Case C-131/12, *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*.

ii *International engagement*

18 Japan signed the International Covenant on Economic, Social and Cultural Rights and the International Covenant on Civil and Political Rights on 30 May 1978. These covenants were ratified on 21 June 1979. The Optional Protocol has not been signed.

19 Japan has not negotiated or signed bilateral or multilateral free trade agreements on personal data transfers with other jurisdictions, and the PPC is not involved in agreements on data protection. No free trade agreements have provisions restricting data transfer.

20 Japan has been an Asia-Pacific Economic Cooperation (“APEC”) Member economy since 7 November 1989 and is a current participant of the APEC Cross-border Privacy Enforcement Arrangement (“CPEA”). As of 28 April 2014, Japan has been part of the Cross-Border Privacy Rules system, with certification having commenced in 2016.¹⁰

21 Japan was granted observer status with the Council of Europe on 20 November 1996, according to the Resolution (96) 37. Japan was granted observer status of the Consultative Committee of Convention 108 on 5 May 2017.

22 Japan has not been recognised by the EU as offering an adequate level of protection under Article 25(6) of Directive 95/46/EC. Although Japan has yet to submit a formal application for a decision from the European Commission on the adequacy of the protection of personal data, the PPC and the Directorate-General for Justice, and Consumers of the European Commission have been in continuous dialogue since 2016 with the intent to establish a framework governing the transfer of personal data between Japan and the EU by early 2018. PPC Commissioner Haruhi Kumazawa and Commissioner Věra Jourová held a constructive meeting in Tokyo on 14 December 2017 with the aim to accelerate work towards achieving mutual adequacy findings as soon as

10 See Ministry of Economy, Trade and Industry, “The Government of Japan Received Approval to Join APEC Cross-Border Privacy Rules System” (News Release, April 2014).

possible in 2018, according to a press release by the European Commission.¹¹

23 Impact of the EU's GDPR on businesses in Japan cannot be clearly determined at present. However, some companies have expressed concerns about the impact of the extraterritorial effects of the GDPR. In that sense, data processing activities by domestic business operators can be affected (see above).

iii *Role of Personal Information Protection Commission*

24 The PPC is the privacy enforcement authority ("PEA") in Japan.

25 The PPC has the authority to establish the Rules mentioned below in relation to cross-border data transfers as prescribed by Article 24 of the APPI, where:

- (a) A third party receiving personal data in a foreign country is in a foreign country or region designated by the PPC Rules as having a personal information protection system and standards equivalent to Japan's.
- (b) A third party receiving personal data in a foreign country has established a system conforming to standards prescribed by the PPC Rules as necessary for continuously taking measures equivalent to those that personal information handling business operators shall take concerning the handling of personal data pursuant to the APPI.
- (c) The principal's (individual's) consent has been obtained to the provision of personal data to a third party in a foreign country.

26 The PPC has provided guidance for interpretation of Article 24, which specifies the restriction on the provision of personal data to a third party in a foreign country: "Guidelines for the Act on the Protection of Personal Information (Provision to a Third Party in a Foreign Country

11 See European Commission – Statement, "Joint Statement by Commissioner Věra Jourová and Haruhi Kumazawa, Commissioner of the Personal Information Protection on the State of Play of the Dialogue on Data Protection" (Press Release Database, 15 December 2017).

Edition)".¹² The PPC has regularly published guidelines for the APPI, including the "General Rules Edition", the "Provision to a Third Party in a Foreign Country Edition", the "Confirmation and Record-keeping Obligation at the Time of Third Party Provision" and the "Anonymously Processed Information Edition" (see below), with the aim to support business operators' activities to implement appropriate and effective measures ensuring the proper handling of personal information. Failure to comply with obligations in the Guidelines will be a breach of the law.

27 As of September 2017, PPC became an Accredited Member at the 39th International Conference of Data Protection and Privacy Commissioners ("ICDPPC") hosted by Hong Kong.

C DEFAULT POSITION, SCOPE AND TERRITORIAL EFFECT

i *Key definitions*

28 Article 2 of the APPI provides key definitions related to this report¹³ as follows:

- (a) "Personal information" means that information relating to a living individual which falls under any of the following items:
 - (i) those containing a name, date of birth, or other descriptions which are stated, recorded or otherwise expressed using voice, movement or other methods in a document, drawing or electromagnetic record,¹⁴ whereby a specific individual can be identified;
 - (ii) those containing an individual identification code¹⁵ (paragraph 1).

12 Professor Graham Greenleaf analyses the adequacy assessments of Japan in "Questioning 'Adequacy' (Pt I) – Japan" (2017) 150 *Privacy Laws & Business International Report* 1 at 6–11.

13 The definitions are partially shortened in order to make them easily understood.

14 Electromagnetic record means a record kept in an electromagnetic form (meaning electronic, magnetic or other forms that cannot be recognised by the human perception).

15 An "individual identification code" means any character, letter, number, symbol or other code prescribed by Cabinet Order (Art 2(2) of the Act on the Protection of Personal Information). The Cabinet Order specifies biometric codes and numbers

(continued on the next page)

Item (i) includes “those which can be readily collated with other information and thereby identify a specific individual”, even if the information concerned cannot be identifiable by itself.

- (b) “Special care-required personal information”¹⁶ is equivalent to “sensitive data”. It means personal information comprising a principal’s (individual’s) race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions, *etc.* This information requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal (individual) (paragraph 3).
- (c) A “personal information database, *etc.*” means those set forth in the following which are a collective body of information comprising personal information:
 - (i) those systematically organised so as to be able to search for particular personal information using a computer;
 - (ii) besides those set forth in the preceding item, those prescribed by Cabinet Order as having been systematically organised so as to be able to easily search for particular personal information¹⁷ (paragraph 4).

The Cabinet Order excludes information which has little possibility of harming an individual’s rights and interests considering the utilisation method (Article 3 of the Cabinet Order).

- (d) A “personal information handling business operator” means a person providing a personal information database, *etc.*, for use in business. However, (i) a central government organisation; (ii) a local government; (iii) an incorporated administrative agency, *etc.*; (iv) a local incorporated administrative agency are excluded (paragraph 5).
- (e) “Personal data” means personal information constituting a personal information database, *etc.* (paragraph 6).

allocated by the Government (a passport number, a pension number, a driver’s licence number, *etc.*) in its Art 1.

16 It is prescribed in Art 2 of the Cabinet Order.

17 *I.e.*, the personal information is organised according to certain rules or a table of contents, index or other arrangement aids retrieval of the personal information.

- (f) “Retained personal data” in this Act means personal data which a personal information handling business operator has the authority to disclose, correct, add or delete the contents of, cease the utilisation of, erase, and cease the third-party provision of, and which shall be neither those prescribed by Cabinet Order as likely to harm the public or other interests if their presence or absence is made known nor those set to be deleted within a period of no longer than one year that is prescribed by Cabinet Order (paragraph 7).

The terms “personal information”, “personal data” and “retained personal data” are distinguished depending on the obligations stipulated in this Act.

- (g) A “principal” in relation to personal information means a specific individual identifiable by personal information (paragraph 8). The terms “individual” or “data subject” may also be used.
- (h) “Anonymously processed information” means information relating to an individual that can be produced from processing personal information so as neither to be able to identify a specific individual by taking action prescribed in each following item in accordance with the divisions of personal information set forth in each said item nor to be able to restore the personal information:
 - (i) Personal information falling under paragraph (1), item (i):
Deleting a part of descriptions, *etc*, contained in the said personal information (including replacing the said part of descriptions with other descriptions, using a method with no regularity that can restore the said part of descriptions).
 - (ii) Personal information falling under paragraph (1), item (ii):
Deleting all individual identification codes contained in the said personal information (including replacing the said individual identification codes with other descriptions using a method with no regularity that can restore the said personal identification codes) (paragraph 9).

ii **Default position**

29 Article 24 of the APPI, which regulates the provision of personal data to a third party in a foreign country, takes the position that international transfers are forbidden as a rule, with exceptions where:

- (a) A third party receiving the provision of personal data in a foreign country is located in a foreign country or region designated by the PPC Rules as a foreign country establishing a personal information protection system recognised to have equivalent standards to that in Japan.
- (b) A third party receiving the provision of personal data in a foreign country has established a system conforming to standards prescribed by the PPC Rules as necessary for continuously taking measures equivalent to those that a personal information handling business operator shall take concerning the handling of personal data pursuant to the APPI.
- (c) The principal's consent has been obtained to the provision of personal data to a third party in a foreign country.

30 A personal information handling business operator in Japan who provides personal data to a third party in a foreign country is subject to Article 24 of the APPI. In addition, pursuant to Article 75¹⁸ of the APPI, Article 24 also applies in those cases where a personal information handling business operator who in relation to supplying goods or services to a person in Japan has acquired personal information relating to that individual handles in a foreign country the personal information, *etc.*

31 The obligations set forth in the APPI cover all personal information handling business operators, irrespective of the type of

18 Article 75 of the Act on the Protection of Personal Information:

The provisions of Article 15, Article 16, Article 18 (excluding paragraph (2)), Article 19 through Article 25, Article 27 thorough Article 36, Article 41, Article 42, paragraph (1), Article 43 and the following Article shall also apply in those cases where a personal information handling business operator who in relation to supplying goods or services to a person in Japan has acquired personal information relating to that individual handles in a foreign country the personal information or anonymously processed information produced by using the said personal information.

business, and apply with no distinction between transfers of data to “controllers” and “processors” or “intermediaries”.

32 The APPI, including Article 24 relating to cross-border data flows, applies to all personal information handling business operators. Exceptions are listed in Article 76, which include press organisations, religious bodies and political bodies, *etc*, using personal information for the purposes stipulated in the said Article.

33 Article 76 applies to all personal information, regardless of domestic or foreign origin, insofar as the prescribed conditions are met. The notion of “personal information” is provided in Article 2 of the APPI.

34 The APPI applies to cross-border transfers of personal data in general, with no specific reference to data in transit.

35 Under the APPI, information that can identify a living individual falls under the definition of personal information, regardless of whether it is pseudonymised or encrypted. Anonymously processed information may be used outside of the original purpose and provided to a third party without the principal’s prior consent. However, the processing method and security control measures must ensure that the information does not identify a specific individual and that the personal information is not restored. The purpose of the provisions is to promote utilisation while ensuring security (Article 2(10), and Articles 36–39). The PPC has published Guidelines and a Report on the handling of anonymously processed information in February 2017.¹⁹

D LEGAL BASIS

36 Article 23 sets out the general principles for transfers of personal data to a third party. It requires a personal information handling business

19 “Report of the Personal Information Protection Commission Secretariat: Anonymously Processed Information – Towards a Balanced Promotion of Personal Data Utilization and Consumer Trust” (February 2017) <<https://www.ppc.go.jp/en/legal/>> (accessed 10 April 2018).

operator to obtain the individual's consent prior to providing their personal data to a third party. "Third party" refers to any person other than the personal information handling business operator providing the personal data or the principal to whom the personal data pertains.

37 There are some exceptions where the principal's (*ie*, the individual's) consent is not required for the transfer under Article 23(1), including:

- (a) when the provision of data is based on laws or regulations;
- (b) when it is necessary to protect a human life, body or property, and it is difficult to obtain a principal's (individual's) consent;
- (c) when there is a special need to enhance public hygiene or promote the sound development of children, and it is difficult to obtain the principal's consent; and
- (d) when there is a need to co-operate with a central government or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs.

38 In addition, there are exceptions to the qualification of a receiving party as a "third party" under Article 23(5):

- (a) when a personal information handling business operator outsources all or part of the personal data processing operations, within the scope of the original purpose of the processing;
- (b) when data are provided in conjunction with business succession by a merger or other reason; or
- (c) in cases where personal data are provided to a specified entity to be utilised jointly with other entities, and when a principal has been informed, or can be deemed to know which data will be utilised jointly by different entities, which entities will be involved, the purpose of this joint utilisation, and the name or appellation of a person responsible for controlling the said personal data.²⁰

20 This definition applies to cases where a group of undertakings jointly use consumer information in order to provide comprehensive services, for example,
(continued on the next page)

39 Many businesses such as cloud service providers or credit card entities engage in international transfers of personal data every day. There are no data on individuals who may opposes such transfers, which are generally acknowledged and accepted.

40 Personal data transfers are not subject to a requirement of notification to, or approval by, the regulator, Government or public entity.

41 There are no other legal bases for international data transfers provided in the law (*eg*, transfer necessary for the performance of a contract in the interest of the individual, or for important business interests).

E DATA LOCALISATION

42 There is no legal obligation to localise personal data in Japan. Although the Foreign Exchange and Foreign Trade Act restricts international transfers of certain kinds of data as a quasi-data localisation regulation, it does not generally serve to restrict the export of personal data.

43 Articles 23 and 24 restrict cross-border data transfers; however, these provisions are not intended to operate as data localisation requirements. These provisions do not distinguish data by type, covering not only “general personal data” but also “special-care required information” (sensitive information). These provisions are applied to “personal data”, not “personal information”.

F DATA TRANSFER MECHANISMS

i *Preliminary issues*

44 Participating in a cross-border data transfer system in Asia operated by multiple countries can enhance the security of personal data and

both the parent and subsidiary companies use customer information, and an employer and a union share employees' information.

protect an individual's rights and interests. It also builds mutual trust among participating parties, facilitating business transactions involving personal data. In addition, if the Asian cross-border data transfer system is developed, Asian countries may be able to gain the trust of the EU that enforces the cross-border data transfer restriction.

45 In data transfers from Japan to a third party in a foreign country, obtaining consent from the principal is the most commonly used mechanism. In practice, many companies obtain the principal's consent prior to disclosing the person's data to a third party. The amended APPI now requires the principal's prior consent for such transfers.

46 The EU Standard Contract Clauses ("SCC") are the most commonly used legal standards for data transfers from the EU to Japan. A few Internet service companies have already applied for or have received recognition under the Binding Corporate Rules ("BCR").²¹

47 In general, compatible or interoperable data transfer instruments are preferable for data transfers between countries. There have been few requests for creating such instruments; however, business operators that have gained recognition under the Cross-Border Privacy Rules ("CBPR") or the BCR might build such data transfer systems. Legal procedures have yet to be enacted to facilitate interoperability for international data transfer. So far, only one Japanese company (Intersect Communications, Inc) has been certified by JIPDEC under the CBPR.

48 Article 24 of the APPI prescribes as one of the conditions for engaging in international data transfers that "a recipient in a foreign country establishes a system conforming to standards prescribed by Rules of the PPC as necessary for continuously taking measures equivalent to those that a personal information handling business operator shall take concerning the handling of personal data pursuant to the APPI". Under this provision, personal information handling business operators can transfer personal data overseas without the individual's consent if

21 The Binding Corporate Rules requested by Rakuten, Inc was first approved by the Luxembourg Data Protection Authority in 26 December 2016. The IJ Group submitted its Binding Corporate Rules to the UK Information Commissioner on 26 October 2016.

adequate guarantees have been put in place, such as entering into an agreement with the recipient.

49 The law provides that the data exporter remains responsible for a breach of personal data by a data importer located in a foreign country when:

- (a) the transfer to a third party located in a foreign country is aimed at outsourcing personal data processing, regardless of the transfer mechanisms adopted by the local data exporter; or
- (b) the transfer mechanism adopted by the local data exporter ensures that a third party receiving the personal data in a foreign country has established a system conforming to standards prescribed by the PPC Rules and equivalent to the requirements for a personal information handling business operator pursuant to the APPI.

Imposing responsibility on the data importer, therefore, does not exempt the data exporter from the obligations prescribed in Article 24.

50 Guidelines for protection of personal data for each of the areas of finance, healthcare and information communication technology, which have specific requirements, have also been published by the relevant Ministries. For instance, Article 16 of the “Guidelines for Protecting Personal Information in the Field of Telecommunications” lays down the rules for disclosing personal data to a third party in a foreign country. The interpretation of it follows the PPC guidelines.²²

51 Furthermore, the APPI recognises the work of Accredited Personal Information Protection Organizations (“APIPOs”), which have specific responsibility in the area of international data transfers (see the CBPR). APIPOs are PPC-recognised private membership organisations, which engage in voluntary activities relating to protection of personal information, such as providing educational information to their member entities and processing disputes relating to personal information. Each

22 Explanatory memorandum to the “Guidelines for Protecting Personal Information in the Field of Telecommunications”. See <http://www.soumu.go.jp/main_content/000507467.pdf> (accessed 10 April 2018).

APIPO further details rules concerning the handling of personal information for its member entities and ensures compliance with the rules by its member entities. There are 44 APIPOs as of 15 December 2017. Their business fields broadly encompass industries such as securities, insurance, banks, credit services, medical services, pharmaceutical services, telecommunication services, mobile content services, marriage agencies, funeral services, security services, driver training and businesses in general. APIPOs usually are not involved in each member entity's international data transfer, however, guidelines laid down by APIPOs follow those crafted by the Ministry of Internal Affairs and Communications, which are also originally based on the PPC guidelines.

52 In addition, in Japan, JISQ1500 has been promulgated as a national standard (industrial standard) by the Japanese Industrial Standards Committee since 1999, which regulates requirements for management systems relating to protection of personal information. This standard is widely known and utilised by private business operators. JISQ15001 was formulated in 1999, following the 1980 OECD Privacy Guidelines and "Guidelines for Protecting Automatically Processed Personal Information in the Private Sector" (originally published in 1997 and amended in 1999 by the Ministry of International Trade and Industry at the time). The PrivacyMark System discussed below requires that criteria based on the JISQ15001 be met. JISQ15001 was amended on 20 December 2017, following the Amended APPI.

53 Japan also has the "PrivacyMark" System, which is a certification of the private sectors' voluntary efforts. The "PrivacyMark" system is operated by a private organisation called JIPDEC. Under the JIPDEC system, a company's handling of personal information is assessed, and if it is found adequate, the company is granted a PrivacyMark to be used in the course of its business activities. The PrivacyMark System enables consumers to easily obtain information on whether a company has earned a PrivacyMark and is thus handling their personal information properly. As of 20 December 2017, 15,560 companies have earned PrivacyMarks. JIPDEC is also the Accountability Agent ("AA") for the APEC CBPR scheme.

ii *Equivalent systems of protection in foreign countries (“white lists”)*

54 As noted above, the APPI authorises transfers of personal data to “foreign countries that have established a personal information protection system with standards equivalent to those of Japan’s regarding the protection of an individual’s rights and interests”.

55 The APPI does not prescribe the standards to decide whether the law of another jurisdiction has established comparable data protection standards, and the data exporter is not authorised to assess the protection level in the destination country by himself. Only the PPC may prescribe that the personal information protection system of a country has equivalent standards to that in Japan regarding the protection of an individual’s rights and interests. The PPC will proceed with an amendment to the Rules based on “Concerning the Future Direction of Commission Rules under Article 24 of the Act on the Protection of Personal Information (APPI (June 16, 2017))”.

56 In considering whether to put specific countries on a “white list”, the PPC makes a judgment based on a comprehensive analysis that considers the impact on personnel expenses as well as cost reductions to the business operator. More specifically, in this document of 16 June 2017, the PPC has presented a series of criteria as “judgmental standards” for the assessment of this level of protection:

- (a) there are statutory provisions or codes equivalent to those relating to the obligations of personal information handling business operators defined under the APPI, and the policies, procedures and systems to enforce compliance with these rules can be recognised;
- (b) there is an independent personal data protection authority, and the authority has ensured necessary enforcement policies, procedures and systems;
- (c) the necessity for a foreign country designation can be recognised as in Japan’s national interest;
- (d) mutual understanding, collaboration and co-operation are possible; and,

- (e) establishing a framework to pursue mutual smooth transfer of personal information, while seeking the protection thereof, is possible.

57 The PPC is also responsible for the assessment of the protection standards in the laws of other jurisdictions. In that capacity, it has been conducting negotiations with the authorities of the EU on the mutual recognition of Japan and the EU as having equivalent levels of data protection. The procedure for such recognition is now being considered by the PPC. At present, the procedure is to be stipulated by the PPC as the PPC Rules on the principle of mutual recognition. The PPC has been engaged in dialogue with the Directorate-General for Justice, Consumers and Gender Equality of the European Commission for mutual recognition between Japan and the EU, and the dialogue is accelerating towards achieving mutual adequacy findings.²³

58 In making such assessments, the PPC is authorised to make decisions of “sectoral adequacy”. The PPC is authorised to recognise that some jurisdictions have established adequate or comparable data protection standards, though such recognition is not necessarily enforced by a “white list”.

iii *Consent as exception to existence of privacy safeguards overseas*

59 Irrespective of the obligation to obtain the principal’s consent for the transfer to be legal, consent may not be used to waive the requirement for existing privacy safeguards in the country of destination.

23 See Personal Information Protection Commission, “Concerning the Smooth and Mutual Transfer of Personal Data Between Japan and the European Union” (4 July 2017) and “Joint Statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission” (14 December 2017).

iv *Other one-off exceptions*

60 There are no other exceptions to the requirement for privacy safeguards by the data importer or in the country of destination accepted by law, for instance when the transfer is necessary for the performance of a contract or for legal proceedings.

v *Contracts*

61 Under Article 24 of the APPI, personal data can be provided to a third party in a foreign country in the same manner as to a domestic third party, “when a third party receiving the transfer of personal information has established a system conforming to standards which rules of the PPC prescribe as equivalent to the requirements on a business operator that handles personal information in Japan”.

62 The “standards prescribed by rules of the PPC” means that (a) actions along with the provisions of the APPI stipulating the obligations of personal information handling business operators are taken between an exporter and an importer of personal data in an appropriate and rational way (*eg*, contracts, notes of certification, memoranda, internal regulations, privacy policies, *etc*), or that (b) an importer of personal data is certified on the basis of an international framework regarding personal information handling (CBPR certification).

63 While SCCs have not been published by the PEA or other competent authorities, a joint adoption of such SCCs would be useful in creating a greater variety of options for the transfer of data internationally.

vi *Cross-Border Privacy Rules*

64 No changes in the law have been necessary after Japan joined the CBPR, nor have specific challenges or legal issues arisen in the process of implementing the CBPR system. However, the Ministry of Economy, Trade and Industry has revised the guidelines outlining the conditions

and procedures for an accredited personal information protection organisation to be appointed as the AA in 2014.²⁴

65 JIPDEC serves as the CBPR AA in the jurisdiction. JIPDEC is required to establish a system to confirm whether a business operator's statements, regulations and operations comply with the requirements of the APEC Privacy Framework and, in the case of disputes, to work with business operators and consumers to settle disputes. The conditions for certification defined by JIPDEC are as follows:

- (a) A business entity who wants to be certified has to agree to be a member of JIPDEC as the APIPO, and comply with the guidelines adopted by JIPDEC.
- (b) The entity applies for the accreditation to JIPDEC by submitting the application form and prior questionnaire. The eight APEC Privacy Principles (notice, collection limitation, uses of personal information, choice, integrity of personal information, security safeguards, access and correction, and accountability) comprise the accreditation criteria.
- (c) JIPDEC examines the application through both the paper and on-site investigation.

66 Primarily, Internet companies have been interested in gaining CBPR certification. Different types of certification depending on the size and profile of companies are authorised.

vii *Certification, trustmarks and privacy seals*

67 A mark or seal is not delivered to a third party even if the law of the country of destination gives the possibility to a company to get its privacy management practices certified by an accredited agent. Certification under the APEC CBPR is a valid means for a data exporter to demonstrate compliance with local cross-border data controls.

24 See <<http://www.meti.go.jp/press/2014/06/20140626004/20140626004.html>> (in Japanese) (accessed 10 April 2018).

68 The law can accommodate a mechanism of mutual recognition of trustmarks or privacy seals delivered in another jurisdiction.

G INTERNATIONAL CO-OPERATION BETWEEN THE PPC AND OTHER PRIVACY ENFORCEMENT AUTHORITIES

i *Co-operation of PPC with foreign PEAs in areas other than enforcement*

69 Article 78 of the APPI enables the PPC to develop operational co-operation with the PEAs in other jurisdictions.

70 Although there are presently no bilateral arrangements with the PEAs of other jurisdictions, the PPC has participated in the APEC CPEA system.

71 Similarly, although there are no specific obligations, Japan considers international trends, *etc*, in interpreting guidance for personal data transfer to a third party in a foreign country. In considering the rules, the PPC is receiving opinions through a public comment process and has received opinions from outside Japan.

ii *Enforcement of cross-border transfer restrictions*

72 While there are no sanctions specifically attaching to the breach of provisions on international data transfer or data localisation, the PPC has enforcement powers for violations of Article 24.

73 However, the PPC has not taken enforcement action against a controller for a breach of Article 24 because no such breach has ever been reported.

iii *International enforcement by PPC*

74 The PPC is party to the Global Privacy Enforcement Network (“GPEN”), APEC CPEA, and the ICDPPC. The PPC has been involved in co-ordinated efforts involving authorities from many countries over the past years – *eg*, the GPEN Sweep.

75 The PPC is not involved in the Unsolicited Communications Enforcement Network (“UCENet”), of which the Ministry of Internal Affairs and Communications and the Consumer Affairs Agency of Japan are members.

76 There are no bilateral arrangements between the PPC and the PEAs of other countries to co-operate in the enforcement of privacy laws. However, the law currently includes provisions for transfer of complaints to PEAs in other jurisdictions,²⁵ disclosure to PEAs in other jurisdictions of information obtained in investigations,²⁶ and assisting other PEAs in cross-border investigations.²⁷ There is also no prohibition on providing information to other enforcement authorities.

77 The PPC published the following interpretation guidelines for the APPI on data transfers: “Guidelines for the APPI (General Rules Edition)” for domestic transfer of personal data, and “Guidelines for the APPI (Provision to a Third Party in a Foreign Country Edition)” for cross-border transfer of personal data. The PPC has not published any policies on data localisation.

78 The PPC’s enforcement role in the APEC Privacy Framework only arises when the violation also violates the APPI.

25 Although there are no explicit articles, “necessary mediation on a lodged complaint,” found in Art 61, item (ii) of the Act on the Protection of Personal Information, administrated by the Personal Information Protection Commission, is interpreted to include transferring complaints to the privacy enforcement authorities in foreign countries when necessary.

26 The Personal Information Protection Commission may provide foreign enforcement authorities with information, recognised as contributing to fulfilling their duties (Art 78(1) of the Act on the Protection of Personal Information), which includes information obtained in investigations.

27 Besides providing the information stated above, international co-operation regarding personal information protection is the responsibility of the Personal Information Protection Commission (Art 61, item (viii)).

Jurisdictional Report

MACAU SAR (THE PEOPLE'S REPUBLIC OF CHINA)

Reporter: **Graça Saraiva**

Lawyer, Associate General Counsel of Sands China Ltd

A INTRODUCTION

1 The Macau Personal Data Protection Act (“PDPA”)¹ was enacted on 29 July 2005 and has been in effect since 29 August 2005. It is noteworthy that the enactment of the PDPA happened three years after the granting by the Executive of the Macau Special Administrative Region of the People’s Republic of China (“Executive” and “MSAR” or “Macau”) of three concessions for the operation of games of fortune and chance in casinos to three different gaming companies² and exactly one year after the opening of the first casino in Macau by Venetian Macau Limited, the first gaming investment project developed by an American company in Asia. The three concessions granted by the Executive were later on extended to six, by means of sub-concession agreements that the Executive authorised each of the gaming concessionaires to grant.³ Apart from one of the gaming concessionaires, all the other gaming concessionaires and sub-concessionaires were ultimately owned by foreign companies.

2 After the handover of Macau from Portugal to the People’s Republic of China in 1999, the granting of the gaming concessions and sub-concessions by the Executive of the MSAR marked the beginning of an unprecedented “boom” of the local economy and the opening of

1 The Macau Personal Data Protection Act is published on the website of the *Macau Official Gazette*. An unofficial English version of the Act is available on the Office for Personal Data Protection website.

2 Sociedade de Jogos de Macau, a subsidiary of STDM, Galaxy Casino, SA and Wynn Resorts (Macao) SA.

3 Venetian Macau Limited, MGM Grand Paradise, SA and Melco PBL Jogos (Macau), SA (today Melco Resorts Entertainment).

Macau to a global economy, with the entering of strong foreign economic interests in the Special Administrative Region. As of the year end of 2016, there were a total of 38 casinos in Macau, now the world's largest gambling hub.

3 The PDPA is inspired by Portugal's legislation, and, as a result, has the closest approach to the European Union ("EU") Data Protection Directive of 1995 than any other country in Asia. The fact that the PDPA is inspired by Portugal's legislation is in itself the biggest challenge that local and foreign businesses in Macau face in terms of compliance with the PDPA, specifically when it comes to cross-border data transfers. This is mainly because Portugal's legislation and the EU Directive were drafted for a space the size of the EU single market where data flow freely and without much constraint. Macau, in turn, is a peculiar jurisdiction: a Special Administrative Region of the People's Republic of China, jurisdictionally autonomous from China and from Hong Kong in application of the "one country, two systems" principle, with *circa* 30 square kilometres, where general services (from minor data processing services to big data cloud services) are outsourced to neighbouring regions and jurisdictions because those services are not generally available in Macau or, when they are available, the offer is limited to one or two providers.

4 In general terms, the PDPA states that cross-border transfers of personal data to a foreign jurisdiction may take place subject to (a) compliance with the PDPA and (b) provided that the legal system in the destination to which the data are transferred "ensures an adequate level of protection" (Article 19). The level of protection of the recipient's jurisdiction is assessed by the Office for Personal Data Protection ("OPDP"), the data protection authority of Macau. If the OPDP considers that the destination to which the personal data are intended to be transferred does not offer an adequate level of protection, the transfer should not take place. There are exceptions to this principle provided in Article 20 of the PDPA, but as we will see below these exceptions should be interpreted restrictively so that the exceptions do not become the rule.

5 There are no public policies to support industry players and/or solutions that have an impact on the cross-border flow of data to and from Macau. Currently there are no guidelines issued by the OPDP in

relation to the transfer of personal data outside of Macau. The materials and literature available in this regard are mainly those published by the European Commission and the Article 29 Working Party.

B GENERAL LEGAL FRAMEWORK OF INTERNATIONAL DATA TRANSFERS

i Existing data privacy protections in MSAR⁴ legislation

6 The PDPA establishes the legal system on the processing of personal data (Article 1).⁵ Processing of personal data is an operation or set of operations which is performed upon personal data, by automatic, semi-automatic or manual means (such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction) (Article 4).⁶

7 The PDPA applies to all forms of personal data processing by automated or semi-automated means as well as non-automated means which form part of or are intended to form part of manual filing systems (Article 3, 1).

8 The PDPA also applies to video and audio surveillance activities, as well as to any other alternative means of capturing image and sound that enables the identification of individuals when the entity that is responsible for the processing of such data resides in Macau or uses a supplier of informatics or telematics networks residing in Macau (Article 3, 3).

4 Macau is a Special Administrative Region of the People's Republic of China ("PRC") and any term referring to national legislation refers solely to legislation from the PRC.

5 Article 1 of the Personal Data Protection Act provides: "This Act establishes the legal system on the processing and protection of personal data."

6 Article 4, 1(3) of the Personal Data Protection Act provides:

Processing of personal data shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

9 The PDPA does not apply to any data processing activities performed by an individual in its domestic activities save for and except if the purposes of the processing is systematic communication or dissemination.

10 The cross-border transfer of personal data is generally subject to all provisions of the PDPA, namely, those regarding the applicable principles,⁷ and specifically to the provisions of Articles 19 and 20.

11 The main principle applicable to cross-border transfer of personal data outside of Macau is defined in Article 19. In accordance with Article 19, cross-border transfers of personal data outside of Macau are subject to all provisions of the PDPA (namely the principles) and may happen where the recipient jurisdiction ensures an adequate level of protection for the personal data to be transferred.

12 Article 20 provides exceptions to the general rule in Article 19, which summarily are the following: (a) where the consent of the data subject has been obtained; (b) where the parties have entered into a contract or are about to enter into a contract and the transfer of data is necessary for the performance of such contract; (c) where there is a vital interest of the data subject to be protected; (d) when the transfer is necessary to defend one's rights in judicial proceedings; (e) where there is a public interest in making the transfer; and (f) if authorised by the OPDP.

13 The sanctions for the breach of the specific provisions that govern the cross-border transfer of personal data contained in Articles 19 and 20

7 Transparency and respect of private life and fundamental rights (Art 2); legality and legitimacy (Art 5, 1(1); personal data shall be obtained for specified and lawful purposes and shall not be processed in any manner incompatible with that purpose (Art 5, 1(2); proportionality (personal data shall be adequate, relevant and not excessive in relation the purpose or purposes for which they are processed) (Art 5, 1(3); personal data shall be accurate and, where necessary, kept up to date (Art 5, 1(3)–(4)); personal data shall not be processed for any other purpose or purposes and shall not be kept for longer than is necessary (Art 5, 1(4)–(5)); appropriate technical and organisational measures should be put in place against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data (Art 15).

are set forth in Article 33 and include fines from MOP\$8,000 to MOP\$80,000. It should also be noted that attempted and negligent acts in breach of the referred provisions are also punishable, as stated in Article 35. In addition, any person (not companies) who intentionally: (a) omits notification or the application for authorisation referred to in Articles 21 and 22; (b) provides false information in the notification or in applications for authorisation for the processing of personal data or makes alterations in the latter which are not permitted by the legalisation instrument; (c) misappropriates or uses personal data in a form incompatible with the purpose of the collection or with the legalisation instrument; (d) promotes or carries out an illegal combination of personal data; (e) fails to comply with the obligations provided for in the PDPA or in other data protection legislation when the time limit fixed by the public authority for complying with them has expired; and (f) continues to allow access to open data transmission networks by controllers who fail to comply with the provisions of the PDPA after notification by the OPDP not to do so, is subject to criminal liability and may be subject to up to one year's imprisonment or a fine of up to 120 days. This penalty shall be increased to double the maximum in the case of sensitive personal data or data relating to suspected illegal activities and criminal or administrative offences. There have been few cases where the OPDP has enforced the provisions on the transfer of personal data outside of Macau.⁸

14 Other laws in Macau⁹ impose confidentiality duties and approval requirements for disclosure (consequently also covering the transfer of data to foreign jurisdictions) of data on certain entities (such as gaming operators and financial institutions). However, only the PDPA addresses the issue of cross-border transfers of personal data specifically.

8 See <<http://www.gdp.gov.mo/index.php?m=content&c=index&a=show&catid=173&id=517>> and <<http://www.gdp.gov.mo/index.php?m=content&c=index&a=show&catid=172&id=573>> (in Portuguese) (accessed 6 April 2018).

9 The legal regime of the financial system; the offshore legal regime; the legal regime of gaming promotion activity.

15 The PDPA is a development of Articles 30,¹⁰ 32¹¹ and 43¹² of the Macau Basic Law (a special law enacted by the People's Republic of China, in force in Macau since 20 December 1999 and which is equivalent to a mini-constitution of the MSAR, subject to the People's Republic of China Constitution).

16 The aim of the PDPA is to protect the individuals' fundamental rights, freedoms and guarantees provided in Article 30 (human dignity, name, reputation, reserve of the intimacy of private and familiar life) and Article 32 (freedom and secrecy of means of communication) of the Macau Basic Law. Article 43 of the Macau Basic Law extends the protection of those rights and freedoms to non-Macau residents.

17 The Macau Civil Code develops some of the referred fundamental rights, namely the right to confidentiality over the intimacy of private life,¹³ the right to confidential communications,¹⁴ the right of protection of personal data¹⁵ and the right over one's image¹⁶ and freedom of speech.¹⁷

10 Article 30 of the of Macau Basic Law states:

The human dignity of Macau residents shall be inviolable. Humiliation, slander and false accusation against residents in any form shall be prohibited.

Macao residents shall enjoy the right to personal reputation and the privacy of their private and family life.

11 Article 32 of the of Macau Basic Law states:

The freedom and privacy of communication of Macau residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communication in accordance with the provisions of the law to meet the needs of public security or of investigation into criminal offences.

12 Article 43 of the of Macau Basic Law states:

Persons in the Macau Special Administrative Region other than Macau residents shall, in accordance with law, enjoy the rights and freedoms of Macau residents prescribed in this Chapter.

13 Macau Civil Code Art 74.

14 Macau Civil Code Art 75.

15 Macau Civil Code Art 79.

16 Macau Civil Code Art 80.

17 Macau Civil Code Art 80.

18 There are no landmark judicial or constitutional decisions in respect of personal data protection in Macau.

ii *International engagement*

19 Macau is a Special Administrative Region of the People's Republic of China with a high degree of autonomy. However, under the "one country, two systems" principle, the authorities retain sole jurisdiction in some areas of competence, which thus fall outside the scope of the autonomy of the MSAR. These areas are foreign affairs, internal defence and national security. Pursuant to Article 13¹⁸ of the Macau Basic Law, the Government of the People's Republic of China is responsible for all foreign affairs in relation to Macau and the Ministry of Foreign Affairs has an office in Macau dealing with these matters.

20 In light of the above, to be applicable in Macau, international agreements or conventions must first be ratified by the People's Republic of China which will then decide whether or not to extend the application of the same to the MSAR. If the application of any international agreement is extended to the MSAR, the MSAR Chief Executive will then order its publication in the Macau *Official Gazette*.

21 On 2 December 1999, the People's Republic of China notified the Secretary of the United Nations about the continued application of the International Covenant on Civil and Political Rights in Macau after the handover of Macau from Portugal to the People's Republic of China. The Chief Executive of Macau then ratified and published the International Covenant on Civil and Political Rights in the Macau *Official Gazette* of 14 February 2001.

18 Article 13 of the of Macau Basic Law states:

The Central People's Government shall be responsible for the foreign affairs relating to the Macau Special Administrative Region. The Ministry of Foreign Affairs of the People's Republic of China shall establish an office in Macau to deal with foreign affairs. The Central People's Government authorizes the Macao Special Administrative Region to conduct relevant external affairs, on its own, in accordance with this Law.

22 Macau is not part of any bilateral or multilateral free trade agreement with other jurisdictions (in Asia or beyond) that cover (sectoral or overall) transfers of personal data between them. Macau is not an observer of the Consultative Committee of Council of Europe Convention 108, nor has it been recognised by the EU as offering an adequate level of protection in application of Article 25(6) of Directive 95/46/EC, or submitted an application to that effect.

23 Given the peculiar structure of Macau's economy described above, it is not envisaged that the extraterritorial effects of the EU General Data Protection Regulation will have a significant impact on the data processing activities of businesses in the Macau.

iii Role of the Office for Personal Data Protection

24 The OPDP in Macau was created by the Chief Executive Order No 83/2007 of the MSAR. It operates independently, although under the supervision of the Macau Chief Executive. The OPDP is the public authority referred to in Article 79, 3¹⁹ of the Civil Code and in various Articles in the PDPA and is the only entity in Macau (with the exception of the Macau courts) with competence to administer the rules of the PDPA. The OPDP is an Observer of the International Conference of Data Protection and Privacy Commissioners ("ICDPPC").

25 The main role of the OPDP is to supervise and co-ordinate the implementation of and compliance with the PDPA. The main functions of the OPDP are²⁰ to process, register and publish the necessary

19 Article 79, 3 of the Civil Code states: "The access to filing systems and informatics registers of personal data in relation to individuals and the combination of personal data is subject, in each case, to the approval of a public authority in charge of monitoring the collection, storage and use of personal data".

20 Articles 19 and 23 of the Personal Data Protection Act – issue opinions about the adequacy of protection of data in foreign jurisdictions; Arts 21 and 23 – receive notifications of processing of personal data and issue authorisations for simplified notifications for certain categories of processing of data; Arts 22 and 23 – issue authorisation for the processing of sensitive data, the processing of credit data, the processing of data for a purpose other than the purpose at the time of the

(continued on the next page)

notifications of personal data processing; to receive, review and decide on requests for authorisations in relation to the matters that are subject to the OPDP's authorisation; to issue opinions based on requests received; to issue authorisations for certain types of required notifications; to receive and handle complaints in relation to the PDPA and to impose administrative sanctions where breaches of the PDPA are detected.

26 As a rule, cross-border transfers of personal data from Macau are subject to the favourable opinion (Article 19) or approval (Article 20, 2) of the OPDP. Exceptions to this general rule are covered by Article 20, 1 of the PDPA, in which case only a notification should be submitted for record to the OPDP.

27 So far, the OPDP has not provided any formal guidance in relation to the implementation of the international transfer provisions. It should be noted, however, that the OPDP is open to informal discussions and guidance to individuals and companies that so request.

28 Furthermore, one must note that the OPDP is actually enforcing these provisions, as a decision released in January 2017 shows.²¹ In practice, it appears that “the increasing reliance on cloud-based services raises particular data protection issues, because some organisations may be hosting personal data in multiple locations outside Macau without realising it”.²²

collection, and the interconnection of data; Art 25 – maintain a public database of data processing exercises that were notified or authorised by the Office for Personal Data Protection and issue an annual report with all opinions and authorisations issued; Arts 26 and 27 – approve codes of conduct; Art 28 – process complaints received; Arts 32, 33, 36 and 43 – impose administrative sanctions (eg, fines).

21 Decision mentioned by Mark Parsons and Louise Crawford in their news brief “Macau: Data Transfer Enforcement Decision “Sends a Warning Signal to Businesses” *Dataguidance* (26 January 2017).

22 Mark Parsons and Louise Crawford, *ibid*.

C DEFAULT POSITION, SCOPE AND TERRITORIAL EFFECTS

i *Default position*

29 The default position of the law is that international transfers of personal data are forbidden unless a series of conditions are satisfied, in particular they are subject to a favourable opinion of the OPDP in respect of the adequacy of the level of protection of the recipient jurisdiction (Article 19, 1). Data transfers may receive a favourable opinion of the OPDP where the OPDP considers that the recipient jurisdiction ensures an adequate level of protection. Whether the level of protection of the country of destination is adequate is assessed on a case-by-case basis by the OPDP, upon request, taking into consideration the specific details of the transfer at stake (Article 19).²³

30 The OPDP may also authorise a cross-border personal data transfer to a jurisdiction that does not offer an adequate level of protection provided the data controller adduces “adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and with respect to their exercise, particularly by means of appropriate contractual clauses” (Article 20, 2).

31 Article 20, 1 provides other exceptions under which data may be transferred to a jurisdiction that does not offer an adequate level of protection, and this time without the approval of the OPDP. These exceptions are analysed in greater detail below.

32 In light of the above, one may conclude that, in practice, the rule in Macau is that the transfer of personal data outside of Macau is always subject to some form of prior control of the OPDP, unless one of the exceptions provided in Article 20, 1 applies.

23 Article 19, 1 of the Personal Data Protection Act provides: “A transfer of personal data to a destination outside the Macau SAR may only take place subject to compliance with this Act and provided the legal system in the destination to which they are transferred ensures an adequate level of protection.”

Article 19, 3 provides: “It is for the public authority to decide whether a legal system ensures an adequate level of protection referred to in the previous number.”

ii *Scope and territorial effect*

33 The international data transfer provisions of the PDPA apply to all data controllers and data processors operating in Macau, provided the data are by any means at any time processed in Macau. Data in transit or that are received in Macau but originated from outside of Macau are also covered by the PDPA.

34 The rules of the PDPA apply to all types of personal data,²⁴ broadly defined in Article 4, 1(1) as:

... any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an indication number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

35 No sectors or companies are exempted from the application of the provisions of the PDPA. The Act applies equally to all data controllers and processors located in Macau, whether in the private or public sector. It applies to the processing of personal data regarding public safety, although this is "without prejudice to special rules in instruments of international law and inter-regional agreements to which the MSAR is bound and specific laws pertinent to public safety and other related regulations" (Article 3, 4).

36 The PDPA does not distinguish between Macau residents and non-residents and its protection applies indiscriminately to "data subjects" generally.

37 The PDPA does not explicitly distinguish between international data transfers to controllers from processors or intermediaries. However, pursuant to Article 15 of the PDPA, whenever a data controller engages a data processor to process the data on his behalf, the data controller shall

24 Name, identification cards, date of birth, address, telephone, e-mail, bank related information, employment related information, criminal related data, credit and solvency data, marital status, consumer habits related data, sensitive data about religious or political beliefs, *etc.*

agree with the data processor, in writing, that the data processor shall process the personal data only upon the instructions of the data controller and the guarantees of the data processor as to the technical security measures and organisational measures governing the processing to be carried out. These requirements weigh on the data controller whether he is located in Macau and engages a data processor located outside of Macau, or where personal data are transferred outside of Macau as a result of such engagement.

38 Anonymised, pseudonymised and encrypted data are excluded from the scope of application only insofar as the recipient of the data is not in possession of other data that would enable it to identify the individuals at stake. This requirement is linked to the definition of personal data under Macau law, which covers any information that identifies or is able to identify an individual.²⁵ Currently, there are no guidelines issued by the OPDP in this regard.

D LEGAL BASIS

39 As mentioned above, there are four distinct, alternative legal bases for the transfer of personal data to a third party outside Macau.

i *Option 1 – General rule (favourable opinion of OPDP)*

40 Data cannot be transferred unless the OPDP issues a favourable opinion in relation to the transfer when it is satisfied that “an adequate level of protection” is assured by the relevant foreign jurisdiction (Article 19 of the PDPA).

25 Article 4, 1(1) of the Personal Data Protection Act provides that “personal data” is:

... any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an indication number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

41 As in EU law, an “adequate level of protection” does not necessarily mean that the foreign jurisdiction must provide no less protection than that provided for by the laws of Macau. An adequate level of protection exists where the legal system of the country of the recipient of the transfer contains rules addressing the same principles that Macau law addresses and should have an appropriate means of enforcing such rules and principles, to an extent deemed sufficient to ensure that the individual to whom the data relates (data subject) has a similar degree of protection.

42 The OPDP determines, upon request for an opinion by the data controller (the entity in charge of the processing of the personal data), whether or not a foreign jurisdiction confers an adequate level of protection for the purposes of transfer of personal data, based on:

- (a) the duration of the processing;
- (b) the nature of the personal data involved;
- (c) the purpose and means of the transfer;
- (d) the legitimacy of the parties involved in the transfer;
- (e) the statutes applicable to the personal data in the country to which the data are to be transferred;
- (f) the project of processing of the personal data;
- (g) the safety measures in place to transfer the data; and
- (h) the policies on technical safety and guidance on the transfer of data.

ii Option 2 – Derogation to general rule (notification to OPDP)

43 An opinion of the OPDP is not required when the personal data are to be transferred to an entity in a jurisdiction that does not offer an adequate level of protection, provided that the OPDP is notified and one of the following applies:

- (a) the data subject gives his or her unambiguous consent (the consent cannot be implied and only applies to the purpose for which the data are to be used as identified in the consent notice (see more below);

- (b) it is necessary for the execution of a contract between the data subject and the data controller, or for due diligence prior to the execution of such contract upon request of the data subject;
- (c) it is necessary for the execution or for entering into a contract to be executed, in the interest of the data subject, between the data controller and a third party;
- (d) it is necessary or legally required for the protection of a Macau important public interest, or for a declaration, exercise or defence of a right in judicial proceedings where the data controller is a plaintiff or a defendant;
- (e) it is necessary to protect the vital interests of the data subject; or
- (f) it is made from a register which according to laws or administrative regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, provided the conditions laid down in law for consultation are fulfilled in the particular case.

These exceptions (in Article 20 of the PDPA) are identical to the exceptions provided for by Article 26(2) of EU Directive 95/46/EC.

iii Option 3 – Safeguards adduced by data controller and data recipient (authorisation by OPDP)

44 Alternatively, the data controller may seek the authorisation of OPDP to transfer personal data to a foreign jurisdiction that does not confer an adequate level of protection, provided that the data controller guarantees adequate safeguard mechanisms with respect to the protection of private life and fundamental rights and freedoms of individuals and with respect to the exercise of such rights, by means of appropriate contractual clauses.

45 This exception is not applicable when the data are to be transferred to a foreign public authority. In the event that the final recipient is a public foreign authority, the transfer of such data should be made in accordance with international treaties or conventions or other legal arrangements governing the provision of such data, which is covered under Option 4 below.

46 Irrespective of which of the above options is chosen, any notifications to, or requests for authorisation or opinion from the OPDP for the purposes referred to above must contain the following information (Article 23 of the PDPA):²⁶

- (a) name and address of the data controller and (if applicable) of its representative;
- (b) purpose of the processing;
- (c) description of the categories of data subjects and categories of the private data in relation to the data subjects;
- (d) recipients or categories of recipients to whom the data may be disclosed/transferred and an explanation of the conditions under which such transfer can be made and how such data can be further used;
- (e) entity in charge of the processing of the data (if it is not the controller);
- (f) interconnection of data (combination of data) (if applicable), *ie*, if the personal data from different sources are being combined;
- (g) length of time the personal data are to be retained;
- (h) conditions under which the data subjects can access or amend their personal data, *ie*, whether the data subject can subsequently amend the data;
- (i) if the data is being transferred to a foreign jurisdiction; and
- (j) general description of the technical and other measures in place to ensure the safety of the processing (measures to protect the data against accidental or illicit destruction, accidental loss, alteration, non-authorised diffusion or access, in particular where the processing involves the transmission of data over a network or by any other means, and against any illicit processing, *etc*).

iv Option 4 – International treaties

47 Under Article 20, 3 of the PDPA, the transfer of personal data to a foreign jurisdiction that constitutes a necessary measure to protect the defence, public security, prevention, investigation and repression of

26 See Office for Personal Data Protection website (Knowledges: Notification/Authorization).

criminal offences and of protection of public health is subject to specific legal provisions or to the instruments of international law and inter-regional agreements to which Macau is a party by virtue of the fact that it is a Special Administrative Region of the People's Republic of China.

48 The transfer of personal data required for the purposes of pending civil judicial proceedings and civil investigations is also subject to specific legal provisions and instruments of international law to which Macau is a party by virtue of the fact that it is a Special Administrative Region of the People's Republic of China.

E DATA LOCALISATION

49 Macau does not follow a forced localisation policy in which national or foreign companies must store personal data within Macau. As seen above, although transfers outside of Macau are subject to a favourable opinion or approval of the OPDP, several exceptions enable the transfer of data without requiring a prior opinion or authorisation by the OPDP.

50 Furthermore, commercial companies are required to physically store their commercial books and records (including personal data) at the head office of the company or in any other place if the board so decides, but in any event in Macau. In the absence of specific regulation differentiating between storage in electronic and non-electronic form, such company data should be stored in Macau. This does not imply, however, that companies may not use cloud-based solutions to facilitate their work and functions, but that such cloud solutions should not be the only repository of the company data.

F DATA TRANSFER MECHANISMS

i *Preliminary issues*

51 The existence of multiple cross-border data transfer regulations offers both benefits and challenges. The major benefit of this variety is that data controllers located in countries that do not offer any protection to the data of their citizens while allowing the storage of data overseas may opt for storing their data in jurisdictions with strong data protection

rules. The major challenge is for data controllers and processors which deal with different systems and requirements to manage complexity, namely, for companies that conduct business in various jurisdictions and groups of companies with companies located in different jurisdictions. The most logical way to overcome the challenges posed by diverging data protection systems between different jurisdictions is to adopt the highest standard of protection available, so as to enable such entities to conduct their business in the various jurisdictions in compliance with different data protection systems.

52 The law imposes an obligation on the exporter to ensure the recipient is bound by legally enforceable obligations regarding the protection of the transferred data when an entity requests for authorisation from the OPDP to transfer data to a jurisdiction that does not ensure an adequate level of protection (Article 20, 2 of the PDPA). The imposition of such obligations on the data recipient may also play a role in OPDP's opinion on the adequacy of the level of protection of a certain jurisdiction (Article 19).

53 In addition, it should also be noted that, irrespective of applicable legal requirements, as a matter of good data governance it is always recommended to do due diligence checks on the data protection practices of the data recipient before the transfer. Agreements should also be made in writing on the guarantees and protections that the data recipient should put in place and comply with in respect of the data that it will receive, when possible. This is particularly relevant when data controllers use cloud providers outside of Macau on the basis of the consent given by the data subjects. In these cases, one must bear in mind that data are transferred outside of Macau because the data subjects consented to such a transfer (but not because they have so requested, nor because the transfer is to protect their direct interests). Therefore, beyond complying with the requirements set forth in Article 15 (for all data controllers that engage data processors to provide data processing services), the parties should agree in writing to any additional guarantees that the recipient party will put in place and comply with while providing the services, so as to ensure the protection of data subjects' private life and freedoms, fundamental rights and guarantees.

54 Generally speaking, under civil law, the data exporter may be held liable if, before having transferred the data, it knew (or should have known) that the data recipient was not in a position to guarantee the security, confidentiality and integrity of the data and the rights and guarantees of the data subjects. Having said that, it should also be noted that any form of liability has to be assessed on a case-by-case basis and depends on various factors.

ii “Adequacy findings” and white lists

55 As already noted, the OPDP may issue opinions in relation to data transfers and whether or not a jurisdiction ensures an adequate level of protection (Article 19, 1). Only the OPDP can decide whether a foreign jurisdiction ensures an adequate level of protection (Article 19, 3). Data exporters are not free to assess the level of protection of a foreign jurisdiction by themselves.

56 The OPDP has never published a list of countries to which it considers that data can be freely transferred.

57 The adequacy of the level of protection of the destination jurisdiction is assessed considering all the circumstances surrounding a data transfer or a set of data transfers. Particular consideration is given to the nature of the data, the purpose and the duration of the proposed processing operation or operations, the place of origin and place of final destination, the rules of law, both general and sectoral, in force in the jurisdiction where the recipient is located and the professional rules and security measures in place at the destination (Article 19, 2). Article 19 of the PDPA does not rule out the possibility of decisions accommodating a sectoral adequacy.

58 The OPDP may formally recognise that some jurisdictions inside and outside Asia have established an adequate level of protection, but the procedure to be followed to that effect is unclear yet. For instance, the provisions of the PDPA do not foresee the possibility of the OPDP formally recognising that certain jurisdictions inside or outside Asia have not established an adequate level of protection.

59 Currently, the OPDP has not made a cost/benefit analysis of the adequacy decisions and white/black lists and there is not enough data to potentially complete such analysis.

iii Consent as exception to existence of privacy safeguards overseas (Article 20, 1(1))

60 As said above, one of the exceptions to the requirement for privacy safeguards overseas is the unambiguous consent of the data subject, which is generally sufficient for a data controller to transfer personal data outside of Macau.

61 In this reporter's experience, obtaining the data subject's consent is the most frequently used data transfer mechanism in Macau. The main factor that weighs on this decision is that, even though this option should be used with certain discretion as it is an exceptional rule, securing the consent of data subjects for the transfer of data is usually the most practical and quickest way to enable a transfer of data outside of Macau.

62 There are, however, three cases in which the data subject's consent is not sufficient to transfer the data outside Macau.

63 The first two exceptions pertain to *sensitive data* and to *credit data*. Pursuant to Article 22, 1 of the PDPA, the processing of sensitive data and of credit and solvency data is subject to the prior authorisation of the OPDP. This requirement implies that any form of processing (including transfer) of these two categories of data is subject to prior authorisation by the OPDP, upon request of the data controller, unless this processing has been authorised by law. For instance, financial institutions and gaming operators may process sensitive data and credit data as these entities are legally obliged to perform background checks on certain patrons mainly for anti-money laundering control purposes and are legally capable of providing credit.

64 The third exception to the ability to rely on the unambiguous consent of the data subject is in relation to the *interconnection or so-called combination of data*. "Combination of data" is any form of processing which consists in the possibility of correlating data in a filing system with

data in another filing system or systems kept by another or other controller for other purposes (Article 4, 1(10)). Unless provided for in a specific legal or administration provision, the combination of data is subject to pre-approval of the OPDP, to be requested solely by the controller, or jointly by the different controllers involved. The combination of data must be necessary for pursuing a legal or statutory purpose and legitimate interest of the data controller, not involve discrimination or a reduction in the fundamental rights and freedoms of the data subjects, be covered by adequate security measures and take account of the type of data to be combined (Article 9).

65 Thus, it is unadvisable for a data controller to transfer personal data outside of Macau with the intent of conducting an interconnection of data by exclusively relying on the data subject's consent. Considering the philosophy of the law and applicable general principles, the consent of the data subject in such a case would not prevail over the statutory provision that states that interconnection is subject to the approval of the OPDP.

66 Irrespective of the obligation to obtain the data subjects' unambiguous consent for the transfer to be legal, consent may be used to waive the requirement for existing safeguards in the country of destination. In any event, as mentioned above, when possible, as a matter of good corporate data privacy governance, it is always recommended that data exporters conduct due diligence checks on the data protection practices and policies adopted by the data recipient before the transfer and adopt adequate contractual clauses between the parties regarding the guarantees and protections that the data recipient should put in place. In practice, even when the country of destination does not guarantee any safeguards for the data to be exported the data exporter may have some degree of control over the safety guarantees adopted by the recipient data, namely, by means of implementing appropriate contractual clauses between the parties.

67 Specifically in relation to the transfers of data to data processors, one should note that Article 15 of the PDPA requires that the controller choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those

measures. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller and that the obligations referred to shall also be incumbent on the processor.

68 As noted, under the general terms of civil liability, the data exporter may be held liable if before the transfer it knows (or should know) that the data recipient is not in a position to guarantee the security, confidentiality and integrity of the data and therefore does not offer an adequate level of protection for the data.

69 The OPDP has not issued any guidelines in this regard.

iv *Other one-off exceptions*

70 As mentioned above, several exceptions set out in Article 20, 1 enable controllers to transfer data to countries with no adequate level of protection, as follows:

- (a) it is necessary for the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken in response to the data subject's request;
- (b) it is necessary for the performance or conclusion of a contract concluded or to be concluded in the interests of the data subject between the data controller and a third party,
- (c) it is necessary or legally required on important public interest grounds, or for the establishment and exercise of defence of legal rights of the data controller in judicial proceedings,
- (d) it is necessary in order to protect the vital interests of the data subject; or
- (e) it is made from a register which according to laws or administrative regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, provided the conditions laid down in law for consultation are fulfilled in the particular case.

71 The OPDP has not issued any guidelines in this regard.

72 However, in the reporter's experience, the most used legal bases for transfers from Macau after consent are probably Articles 20, 1(1), (2) and (3), which allow transfers of personal data to non-adequate countries when these transfers are necessary for the performance or execution of contracts.

73 The transfer of personal data that constitutes a necessary measure to protect the defence, public security, for the prevention, investigation and repression of criminal offences and for the protection of public health shall be governed by specific legal provisions or by the instruments of international law and inter-regional agreements to which Macau SAR is a party.

v Contracts

74 It is compulsory for the data exporter to conclude a contract with the data importer if the data importer is to process personal data on behalf of the data controller (Article 15, 3). The controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out and must ensure compliance with those measures (Article 15, 2).

75 The contract (or other legal act binding the processor to the controller) shall stipulate in particular that the processor shall act only on instructions from the data controller and that the data processor is under the obligation to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other forms of unlawful processing. Having regard to the state of the art and the cost of implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

76 In the case of processing of sensitive data or data about suspected illegal activities, criminal and administrative offences, the following

additional measures shall be stipulated in the contract with the data processor: (a) unauthorised persons shall not enter the premises used for processing such data (control of entry to the premises); (b) data media shall not be read, copied, altered or removed by unauthorised persons (control of data media); (c) unauthorised input and unauthorised obtaining of knowledge, alteration or elimination of personal data input shall be prevented (control of input); (d) automatic data processing systems shall not be used by unauthorised persons (control of use); (e) authorised persons shall only access data covered by their level of authorisation (control of access); (f) guarantee the checking of the bodies to whom personal data may be transmitted (control of transmission); (g) guarantee that it is possible to check *a posteriori*, in a period appropriate to the nature of the processing, the establishment in the regulations applicable to each sector of which personal data are input, when and by whom (control of input); (h) in transmitting personal data and in transporting the respective media, unauthorised reading, copying, alteration or elimination of data shall be prevented (control of transport).²⁷

77 The OPDP has not issued further guidelines in this regard.

78 The contract concluded between the data exporter and importer must contain a third-party beneficiary clause to benefit the individual whose data are transferred otherwise third parties do not have enforcement contractual rights under the contract.

79 The OPDP has not published Standard Contractual Clauses for the transfer of personal data but those approved by the European Commission may be used as a reference.

27 Article 16, 1 and 2 of the Personal Data Protection Act. In addition, pursuant to Article 16, 3 and 4:

3. The systems must guarantee logical separation between data relating to health and sex life, including genetic data, and other personal data.

4. Where circulation over a network of the data referred to in Article 7 may jeopardise the fundamental rights, freedoms and guarantees of their data subjects the public authority may determine that transmission must be encoded.

80 The joint adoption of Standard Contractual Clauses by several Asian countries would be useful to all companies, especially with respect to cloud service providers and e-commerce providers.

vi Cross-Border Privacy Rules

81 Macau has not joined or lodged a Notice of Intent to participate in the Asia-Pacific Economic Cooperation (“APEC”) Cross-Border Privacy Rules (“CBPR”) system and there is no CBPR Accountability Agent.

vii Other data transfer instruments (certification, trustmarks and privacy seals, codes of conduct, etc)

82 There are no other data transfer mechanisms provided for in the law apart from the ones referred to above. For instance, the law in Macau does not allow a company to get its privacy management practices certified by an accredited agent and be delivered a mark or seal upon positive findings.

83 Regarding codes of conduct, Article 26 of the PDPA provides that the OPDP shall encourage the implementation of professional and sectoral codes to contribute to the proper implementation of the provisions of the PDPA, enhance efficiency and self-regulation, and to exercise and protect the basic privacy rights, taking into account the specific features of the various sectors. Professional associations and other bodies representing other categories of controllers which have drafted codes of conduct may submit them to the OPDP for registration. Such registration shall be made if the OPDP considers the draft to be in compliance with the PDPA and other regulations in force in the area of personal data protection. The registration of codes of conduct has the effect of a declaration of its lawfulness, but does not have the nature of a legal provision or a statutory regulation (Article 27).

84 However, it is not known if the existence of codes of conduct adopted by the data recipient in the country of destination is taken into account by OPDP as a positive factor in its assessments of transfer authorisation requests on the basis of Article 20, 1(1) of the PDPA.

G INTERNATIONAL CO-OPERATION BETWEEN OPDP AND OTHER PRIVACY ENFORCEMENT AUTHORITIES

i *Co-operation with foreign privacy enforcement authorities in other areas of enforcement*

85 The Macau PDPA currently does not include provisions that enable the OPDP to develop operational co-operation with the privacy enforcement authorities in other jurisdictions.

86 The OPDP does not have any bilateral or multilateral arrangement with the PEAs of other jurisdictions.

87 The OPDP is only subject to the law when making its decisions.

ii *Enforcement of cross-border transfer restrictions*

88 The following are sanctions specifically attached to the breach of provisions on international data transfers:

- (a) Entities that do not notify the OPDP within eight days after starting to treat personal data commit an administrative offence subject to:
 - (i) individuals – fine from MOP\$ 2,000 up to MOP\$20,000;
 - (ii) companies – fine from MOP\$10,000 up to MOP\$100,000.
- (b) Entities that do not request the relevant authorisation from the OPDP as referred hereinabove commit an administrative offence subject to:
 - (i) individuals – fine from MOP\$4,000 up to MOP\$40,000;
 - (ii) companies – fine from MOP\$20,000 up to MOP\$200,000.

The transfer of personal data abroad not in compliance with the applicable provisions is considered an administrative offence and subject to a fine from MOP\$8,000 up to MOP\$80,000.

iii *Criminal offences and penalties*

89 Companies are not subject to criminal liability, but the individuals that commit any of the offences described below are subject to imprisonment for up to 120 days or to the payment of a fine:

- (a) intentional omission of the notification to the OPDP for the processing of personal data or of the request for authorisation where it is necessary;
- (b) intentional provision of false information in the notification or in the authorisation request submission;
- (c) intentional deviation or usage of personal data in a way that is incompatible with the purpose in accordance with which the data was initially collected;
- (d) intentional promotion or execution of illegal combination of personal data;
- (e) intentional non-compliance with legal provisions on protection of personal data after being given a deadline by the OPDP to comply with such legal provisions; and
- (f) intentional maintenance of access to open data transmission networks to entities that do not comply with the law on personal data protection, after being notified by the OPDP not to do so.

Where the personal data is related to sensitive information or to suspected illicit activities or administrative or criminal offences, the penalties mentioned above will be doubled.

90 The OPDP is the administrative body with exclusive competence to investigate and make decisions regarding all provisions of the PDPA and may impose sanctions. The OPDP does not have an enforcement policy in place. The PDPA has imposed sanctions on entities in Macau for acts that were deemed to be illegal transfer of personal data outside of Macau.

iv *International enforcement by OPDP*

91 The OPDP belongs to the Asia Pacific Privacy Authorities (“APPA”) and Global Privacy Enforcement Network (“GPEN”), two international networks that may adopt guidance or develop enforcement actions jointly.

92 The PDPA does not include any provisions for the transfer of complaints to other jurisdictions or disclosure to PEAs in other jurisdictions of information obtained in investigations, assisting other PEAs in cross-border investigations or a prohibition to provide other

enforcement authorities with information or assistance. However, it should be noted that the transfer of personal data that constitutes a necessary measure to protect the defence, public security, prevention, investigation and repression of criminal offences and for the protection of public health is governed by specific legal provisions or by the instruments of international law and inter-regional agreements to which Macau is a party.

93 The OPDP has not issued an enforcement policy on data transfers or data localisation requirements.

94 The OPDP participates in the GPEN, but does not participate in the following: GPEN Alert, APEC Cross-border Privacy Enforcement Arrangement, ICDPPC Enforcement Cooperation Arrangement or Unsolicited Communications Enforcement Network.

95 The OPDP does not perform an enforcement role under the APEC CBPR system; nor does it have any bilateral arrangements with PEAs of other countries to co-operate in the enforcement of privacy laws.

96 The OPDP has never undertaken a joint investigation with any other PEA in the same country or in a foreign country, but has already provided assistance in an investigation being undertaken by a PEA from another country, has transferred a complaint to a PEA from another country and has received a complaint transferred to it from a PEA in another country. The OPDP has never taken an enforcement action jointly with one of its foreign counterparts, nor issued common findings against a foreign data controller based in multiple jurisdictions.

Jurisdictional Report MALAYSIA

Reporter: **Abu Bakar Bin Munir***

Professor, Faculty of Law, University of Malaya

A INTRODUCTION

1 Due to significant advances in information and communication technologies (“ICT”), it has become easier to share data with people around the world in just a “click” by using various technologies, the Internet, intranet or interconnected databases. In our everyday life, we disclose our personal data by using online services, such as online banking, e-government and e-commerce.¹

2 The dependence on ICT is even stronger in the case of multinational corporations (“MNCs”),² who are required to provide a wide array of data obtained from their customers or employees to their numerous offices operating around the globe. In order to gain a competitive edge, these companies seek to provide optimum benefits and 24-hour customer services to their customers; for instance, technical support, customer service, consumer databases and central human resources are being positioned globally in different offices of the corporate group. Moreover, these days, companies very often outsource

* The reporter addresses his most sincere thanks to the Commissioner of Personal Data Protection of Malaysia for the feedback provided by her office on the report, and to the agents of the companies interviewed for the purposes of this study for their time.

1 Y D Wang & H H Emurian, “An Overview of Online Trust: Concepts, Elements, and Implications”. (2005) 21(1) *Computers in Human Behavior* 105.

2 P Cooke & O Memedovic, “Strategies for Regional Innovation Systems: Learning Transfer and Applications” Vienna: United Nations Industrial Development Organization Policy Paper, 2003.

to offshore companies' different services³ such as call centres, payroll management, accounting services, credit card application, bill processing, *etc.* By doing so, they save on investment in expensive infrastructure for these services and on the cost of labour.

3 For all these services to function, internally or when outsourced, databases containing data of employees, customers or business partners from all around the world are created. All affiliate companies have access to such databases, and can usually send, view and/or download the contained data. In practice, this means that two-way data traffic between the database and each of the countries that the company is located in takes place. As a result, data are geographically "moved" among different countries, or even continents.

4 As a leading financial hub of the Association of Southeast Asian Nations ("ASEAN"), Malaysia has boosted its ICT infrastructure and markets to attract foreign investments⁴ and achieve significant economic growth. Cloud companies and global data centres such as Google, Microsoft, Amazon, HP, Equinix, Global Switch, Savvis and many others have either invested or are in the midst of investing in Malaysia. The new government policies are also attracting more investments from MNCs in other sectors. More MNCs means more cross-border data transfers. However, there are still barriers to cross-border data flows, in Malaysia and worldwide.

5 Although cross-border data flows are vital for firms, individuals and different organisations, governments need to regulate the free movement of information traversing borders in numerous ways.⁵ Restricting such data flows would require legal provisions on data collection and

3 L M Ellram, W L Tate & C Billington, "Offshore Outsourcing of Professional Services: A Transaction Cost Economics Perspective" (2008) 26(2) *Journal of Operations Management* 148.

4 R Gholami, S Y Tom Lee & A Heshmati, "The Causal Relationship Between Information and Communication Technology and Foreign Direct Investment" (2006) 29(1) *The World Economy* 43.

5 A L Newman, "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive" (2008) 62(1) *International Organization* 103.

localisation, with regulations restricting the ability to move and process personal data across borders. The prime objectives of adopting such laws on cross-border data transfer are to prevent the abuse of personal data, to ensure that data are kept securely and to ensure that data are accurate. The utmost goal of a reliable regulatory framework, however, is to preserve consumer interests and rights.

6 Though there are regulatory barriers, the speed of data transfers across the Internet continues to increase. As companies and individuals develop faster and more efficient ways of facilitating international digital transfers, the need to agree on a uniform method of regulating the countless number of cross-border data transfers becomes even more pressing.⁶ The debate over how to regulate international data transfers brings with it a multitude of other salient topics to consider, such as how to store, process and access big volumes of data from around the globe. This report will focus on Malaysian data legislation and how data privacy and transfer standards in ASEAN countries measure up to them.

B WHAT ARE CROSS-BORDER DATA TRANSFERS?

7 Every time a credit card is swiped at a store, a plane ticket is purchased, or a GPS navigation device is used, personal data is transferred. As everyday transactions in business, politics and our personal lives become increasingly dependent on digital technology and the Internet, our personal information becomes more widely available and, therefore, increasingly vulnerable. Giving away personal information like full names, birthdates, addresses and phone numbers to unknown third parties has been normalised to a point where we no longer think twice about volunteering our personal information when prompted online.

8 Whenever someone creates an account on a social networking website or downloads a messaging app onto their smartphone, they are not only sharing private information with the people they connect with,

6 K Alboukrek, "Adapting to a New World of E-Commerce: The Need for Uniform Consumer Protection in the International Electronic Marketplace" (2003) 35 *George Washington International Law Review* 425.

but also giving companies' the right to store and use their private information as outlined in their user terms and conditions.

9 Companies engaged in cross-border data transactions transfer data from one point to another, often using multiple nodes of data transit points scattered throughout the world to relay the information in the process. The Internet automatically locates and funnels data through the closest available data node, switching directions and transferring packets of data in seconds.⁷ These data nodes are located in different countries and are shared by Internet users all over the world.⁸ Because origin and destination points are scattered across every corner of the globe, one single piece of legislation cannot account for all the necessary measures that need to be in place in order to enforce the protection and privacy of transferred data. However, having disjointed or overlapping legislation, especially when dealing with an issue with drastic international repercussions, further exacerbates the already difficult problem of trying to figure out a way of dealing with the novel challenges of handling data and emerging digital technologies.

10 The safe and secure storage of data is just as important as the safe and secure transfer of data. As data travel from point A to point B, data handlers must also ensure that the personal data stay private before, during and after the transfer. Recently, Malaysian authorities have arrested a hacker accused of stealing the personal information of more than 1,000 US security officials and giving it to the Islamic State ("IS") group in Syria.⁹ The hacker is accused of exposing national identification numbers, addresses and phone numbers, which the Associated Press verified.¹⁰

7 K Alboukrek, "Adapting to a New World of E-Commerce: The Need for Uniform Consumer Protection in the International Electronic Marketplace" (2003) 35 *George Washington International Law Review* 425.

8 P Danese, P Romano & S Boscari, "The transfer process of lean practices in multi-plant companies" (2017) 37(4) *International Journal of Operations & Production Management* 468.

9 "Malaysia Arrests Hacker for Allegedly Providing US Security Data to Islamic State" *ABC News* (15 October 2015).

10 "Malaysia Arrests Hacker for Allegedly Providing US Security Data to Islamic State" *ABC News* (15 October 2015).

11 The unconcerned reactions by the Government often mislead the general population about the dangers of data privacy breaches. By downplaying the severity of the consequences of privacy violations, the average citizen remains unaware of how rampantly and frequently his personal data are exposed. In addition, people do not realise how much they rely on digital technology to go about their daily lives. Perhaps, because of this lack of awareness, people are generally loath to demand greater privacy protections from their political leaders.

12 There are numerous sectors that illustrate how vital data transfers are for business and personal health. One key sector is that of digital medical devices,¹¹ which store personal and health data for diagnostic and treatment purposes. For example, devices that are too large to transport for repairs and maintenance are accessed by authorised repair personnel remotely, who gain access to the personal and health data of patients stored on these medical devices. Storing such sensitive information about patients is often viewed with suspicion as the engineer or repair crew handling medical device repairs are usually not legally authorised to access such sensitive data. In more extreme cases, patient data can be leaked or sold¹² to the pharmaceutical industry for marketing and research. This area is important for Malaysia, which has positioned itself as a medical device design and manufacturing hub.

13 Another controversial sector pertaining to the storage of and access to sensitive data is the energy sector.¹³ International oil and gas companies (“IOCs”) collect and store geographic and geopolitical data on a large number of pipeline, upstream and downstream facilities in order

11 R J Wood, *et al*, *US Patent No 9,642,517* (Washington, DC: US Patent and Trademark Office, 2017).

12 See Malaysian Investment Development Authority, “Medical Devices” <<http://www.mida.gov.my/home/medical-devices/posts/>>, and Danielle Kirsh, “Paramit Opens Medical Device Design and Manufacturing Hub in Malaysia” <<https://www.medicaldesignandoutsourcing.com/paramit-opens-medical-device-design-manufacturing-hub-malaysia/>> (both accessed 10 April 2018).

13 D Schweer & J C Sahl, “The Digital Transformation of Industry – The Benefit for Germany” in *The Drivers of Digital Transformation* (F Abolhassan ed) (Springer International Publishing, 2017) at pp 23–31.

to optimise their exploration, extraction and export operations.¹⁴ The ability to conduct proper assessments requires storing and processing data on topography, climate, politics (*ie*, cases of riot, attack or sabotage) and key technical data that belong to other countries, down to data on energy consumption in individual homes. This begs the questions of whether such key strategic data should be accessed or stored by private companies and how privacy protection safeguards can prevent these companies from selling such information to other third parties or foreign intelligence agencies that were not the intended recipients of such data.

14 Similar debates occur in the insurance sector, where foreign insurance companies store and process the data of beneficiaries in other countries.¹⁵ Malaysia, which stands as a leading destination for the establishment of shared services and outsourcing (“SSO”) hubs,¹⁶ is concerned by this issue. Insurance companies usually cite the need to back up beneficiaries’ personal data in a secondary location abroad to ensure efficient processing of data and the physical protection of the data.¹⁷ In other words, if indigenous data centres are harmed physically, such as through natural disasters like hurricanes and tornadoes, data redundancy ensures that copies of the same information are readily available to access at other locations.

15 The aforementioned examples and many other cases of data processing and storage have brought about the need for governments to step in and establish certain rules and regulations – in Malaysia, the Personal Data Protection Act. Such intervention serves two purposes:

14 L Herkenhoff, *A Profile of the Oil and Gas Industry: Resources, Market Forces, Geopolitics, and Technology* (Business Expert Press, 2013).

15 L Baker, “The Impact of the General Data Protection Regulation on the Banking Sector: Data Subjects’ Rights, Conflicts of Laws and Brexit” (2017) 1(2) *Journal of Data Protection & Privacy* 137.

16 Address by Mr Mohd Razif bin Abd Kadir, Deputy Governor of the Central Bank of Malaysia, at the Shared Services and Outsourcing in the Financial Sector – A Joint Forum by Bank Negara Malaysia and the Multimedia Development Corporation (Kuala Lumpur, 13 November 2007).

17 Address by Mr Mohd Razif bin Abd Kadir, Deputy Governor of the Central Bank of Malaysia, at the Shared Services and Outsourcing in the Financial Sector – A Joint Forum by Bank Negara Malaysia and the Multimedia Development Corporation (Kuala Lumpur, 13 November 2007).

one, to protect citizens' privacy, and two, to protect sensitive national data that may be defined as "strategic data". The debate on restriction versus freedom of data flows is polarised along two lines. The first is that governmental restrictions are necessary to prevent abuse and mishandling of such data, preventing privacy abuses and ensuring the protection of sensitive strategic data. The second is that excessive governmental restrictions on data flows impair business speed – the same way that high tariffs and excessive border controls stifle trade – and hurt a country's business competitiveness. Indeed, companies that feel too much intrusion into businesses' handling of data will cause them to be inclined to move their businesses to countries with fewer restrictions on collecting, processing and storing data. To that end, restrictions on data flows have a direct impact on business and investment.

C BARRIERS TO CROSS-BORDER DATA FLOWS

16 Based on what has been reported by companies, interviews and studies done in the course of this study, two types of restrictions are the most common – data localisation requirements and data protection regulations. Other barriers to cross-border data streams, such as intellectual property regulation and Internet censorship, will not be considered in this report.

i *Local storage and forced localisation*

17 For companies, legal requirements to either locally store data or utilise local data servers only¹⁸ have been distinguished by some as having the most potential distortion among the trade measures which are currently being applied.¹⁹ The Malaysian government has not implemented requirements mandating use of onshore providers, but

18 F Malomo, & V Sena, "Data Intelligence for Local Government? Assessing the Benefits and Barriers to Use of Big Data in the Public Sector" (2017) 9(1) *Policy & Internet* 7.

19 R Moshell, "And Then There Was One: The Outlook for a Self-regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection" (2004) 37 *Tex Tech L Rev* 357.

rather provides inducements to attract foreign and domestic investors to the Multimedia Super Corridor, a government scheme to foster the growth of research, development and other high technology activities in Malaysia.²⁰

18 Concerns regarding personal data and protecting data from misuse are two motivations behind data localisation requirements. The underpinning argument is that if data are stored locally, they will be much safer and governments will be in a better position to prosecute if data privacy is infringed.²¹ Usually, the intent behind forced localisation is to encourage production, investment or the setup of foreign enterprises. Normally, safeguarding personal information is not the sole purpose of this sort of laws or regulations – they seldom even have a protectionist foundation.²² Many countries, both developing and developed, are either enforcing or intending to enforce such requirements.

19 Forced localisation provisions decree that within a country, a data centre should be established by foreign enterprises as a requirement to be authorised to render specific digital services within that country. Vietnam is proceeding to enforce a law that would need companies' data centres, web search portals and cloud computing services to be hosted within the country. Indonesia also has a regulation of the same sort which would demand all data carriers, including foreign banks, and mobile phone providers performing in the country, to build local data servers within the country.

20 When crossing a country's boundary, several restrictions on the procedure and storage of data are implied as *per* the requirements of local data storage. For instance, China, Brunei and India have laws which demand that data generated inside the country should be stored on

20 See "Malaysia – 4-Industrial Policies" <<https://www.export.gov/article?id=Malaysia-Industrial-Policies>> (accessed 10 April 2018).

21 A Savelyev, "Russia's New Personal Data Localization Regulations: A Step Forward or a Self-imposed Sanction?" (2016) 32(1) *Computer Law & Security Review* 128.

22 C Cimino, G C Hufbauer, & J J Schott, "A Proposed Code to Discipline Local Content Requirements" (2013) *Policy Brief* 14.

servers within the country. Consequently, such laws prohibit public organisations from using foreign digital service providers (for example, cloud services) in situations where personal information could be stored in or obtained from a foreign country.

21 Furthermore, numerous countries associate forced localisation requirements with local data storage requirements. For instance, India has proposed standards asking companies to place a portion of their ICT infrastructure inside the country. At the same time, this law would demand that the data of government organisations, Indian citizens and firms not be transferred out of the country.

ii *Personal data and data protection regulation*

22 As opposed to local data storage and forced localisation which are currently only enforced in a small number of countries, laws regulating personal data are more common.²³ The large volume of personal data that is obtained, used and transported to other countries, including that of third parties, raises concerns regarding personal data and control over one's own data. As the volume of personal data processed increases, so does the concern from individuals regarding how their personal data are being used.

23 As of 2016, some sort of privacy legislation and data protection which limits the application and transfer of either personal or any sensitive data had been adopted by more than a hundred countries.²⁴ This kind of regulation is meant to rein in risks of abuse of personal information and to preserve individuals' right to information privacy. Companies across different industries are obliged to comply with the aforementioned laws, which create difficulties arising from restrictive or burdensome laws as well as differing legal frameworks between countries, which in turn generate higher compliance costs and unpredictability for firms.

23 See Professor Graham Greenleaf, *Asian Data Privacy Laws, Trade & Human Rights Perspectives* (Oxford University Press, 2014) (updated 2017).

24 V Haufler, *A Public Role for the Private Sector: Industry Self-regulation in a Global Economy* (Carnegie Endowment, 2013).

D ROLE OF GOVERNMENT IN DATA PRIVACY PROTECTION

24 Not only private companies may abuse or mishandle personal data of individuals. Perhaps an even more important question is how much personal data on their citizens governments should collect, store and process, as well as what kind of legal precautions should be taken to protect privacy. In order to render citizenship services, bureaucracy and security more efficient, governments have also begun collecting, storing and processing citizens' personal data, such as address, national identity, financial and legal background information.

25 The rationale, scope and legal framework for data collection are widely disputed among countries. However, many also wrestle with whether countries that lack the sufficient technical infrastructure to protect citizens from cyber-attacks should be collecting personal data on their citizens in the first place.

26 One of the oldest debates in politics, freedom-versus-security,²⁵ is perhaps more relevant today in the debate between government surveillance and individual privacy. Malaysia has not escaped this debate since the passage of the National Security Council Act in 2016.²⁶ Since the 1990s, an increasing number of countries have adopted data protection and privacy laws or regulations. However, commonly shared definitions for personal data, data collection and data processing differ, rendering these laws incompatible and geared towards disparate outcomes. An important analytical problem arising from these differences is how to approach the issue of data collection – how much data should be collected by governments and private companies and which legal and ethical constraints should be imposed upon them to prevent collection and processing abuses? Moreover, who does data belong to?

25 A Etzioni, *How Patriotic is the Patriot Act?: Freedom Versus Security in the Age of Terrorism* (Routledge, 2005).

26 Act 776.

27 Governments, companies and even computer games collect and store personal data,²⁷ which in turn, can be accessed, processed and accessed surreptitiously by government surveillance agencies. While the digital age has brought about new freedom frontiers and liberty zones for citizens, it has also provided governments with better tools to respond positively or negatively to the growing scope of electronic liberties. The emergence of multiple data collection bodies and institutions and their overlapping and sometimes competing data storage policies bring in the question of what happens if personal data are lost, damaged or misused.

28 Regardless of the source or purpose of the stored data, emerging markets like Malaysia must align their data protection legislation with the standards of their trading and political partners. As a South-Asian country and ASEAN member, Malaysia must shape its laws to fit the mould of Asia. With the Personal Data Protection Act 2010²⁸ (“PDPA”), Malaysia has started to take steps toward reforming its either outdated or non-existent data protection laws to better respond to the challenges of the 21st century.

E OVERVIEW OF THE MALAYSIAN PERSONAL DATA PROTECTION ACT 2010

29 In May 2010, the Malaysian Parliament enacted the Personal Data Protection Act 2010 (PDPA and on 2 June 2010 the PDPA received the Royal Assent.²⁹ Through the method of notification in the *Government Gazette*, on 15 November 2013, the PDPA came into force after a three-month sunrise period on 15 February 2014. The European Data Protection Directive and the Malaysian PDPA have a lot in common.

27 C Mundie, “Privacy Pragmatism; Focus on Data Use, Not Data Collection” (2014) 93 *Foreign Affairs* 28.

28 Act 709.

29 E L Yong Cieh, “Personal Data Protection and Privacy Law in Malaysia” in *Beyond Data Protection* (N Ismail & E L Yong Cieh eds) (Springer Berlin Heidelberg, 2013) at pp 5–29.

i *Territorial scope of PDPA*

30 Generally, the PDPA will apply to data users in three circumstances:

- (a) Firstly, where the data user is established in Malaysia and the data user processes data, whether or not in the context of the establishment.
- (b) Secondly, when the processing is done by any person employed or engaged by the data user established in Malaysia.
- (c) Thirdly, when the data user is not established in Malaysia, but uses equipment in Malaysia to process personal data.

31 A data user is considered as “established in Malaysia” when the user is “an individual whose physical presence in Malaysia shall not be less than one hundred and eighty days in one calendar year”, a body incorporated under the Companies Act 1965, a partnership or other unincorporated association formed under any written laws in Malaysia, and any other person who maintains in Malaysia an office, branch or agency through which he carries on any activity, or a regular practice (section 2(4) of the PDPA).

32 Further, it does not apply to the processing of personal data outside of Malaysia unless that data is to be processed further in Malaysia (section 3(2) of the PDPA).³⁰

ii *Organisations, data and operations covered by PDPA*

33 The PDPA states that the Act shall apply to any person who, alone or jointly with others, processes or any person who has control over or authorises the processing of any personal data in respect of commercial transactions (section 2).

30 E L Yong Cieh, “Personal Data Protection and Privacy Law in Malaysia” in *Beyond Data Protection* (N Ismail & E L Yong Cieh eds) (Springer Berlin Heidelberg, 2013) at pp 5–29.

34 Two sectors are wholly exempted from the scope of the PDPA:

- (a) Malaysian State and Federal authorities; and
- (b) credit reporting agencies constituted under the Credit Reporting Agencies Act 2010,³¹ regarding the processing of personal information for the sole purpose of the activities under this Act. However, the latter are subject to strict conditions on the processing of personal information, and individuals are granted rights of access, correction, deletion, *etc* (sections 22 to 31, “Conduct of Business of Credit Reporting Agencies”).

35 “Personal data” is defined as any information in respect of a commercial transaction, which:

- (a) is processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
- (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or
- (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

36 Personal data is further defined as “information which relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject” (section 4 of the PDPA). The Personal Data Protection Commissioner (“Commissioner”) has not adopted specific guidance on the notion of personal data or anonymised data. However, codes of conduct occasionally refer to anonymisation as a security measure that can be taken when personal data are no longer necessary in accordance with professional standards and best practices, *eg*, in the life insurance industry.³²

31 Act 710.

32 Code of Practice on Personal Data Protection for the Insurance and Takaful Industry in Malaysia Art 11 (Retention Principle).

37 The PDPA also differentiates between sensitive personal data and personal data, with stricter conditions applying to the conditions of processing of the former.

38 As mentioned, the PDPA monitors individually identifiable data which are obtained in the course of a “commercial transaction”.³³ “Commercial transactions” are defined in the last paragraph of section 4 of the PDPA as:

... any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agencies Act 2010.

The Personal Data Protection Department has considered that employment-related data would fall within the scope of “commercial transactions” and be subject to the PDPA.

39 “Processing” is defined to mean collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including the organisation, adaptation or alteration of personal data, the retrieval, consultation or use of personal data, the disclosure of personal data by transmission, transfer, dissemination or otherwise making available, or the alignment, combination, correction, erasure or destruction of personal data.

iii *Personal Data Protection Principles (sections 5 to 12 of PDPA)*

40 The PDPA asserts seven Personal Data Protection Principles to be complied with when processing personal data. If the data user does not comply with any of the Principles and is found to be in breach of the PDPA, the punishment involves payment of fines and/or imprisonment.

33 L M Marvin, “Conducting US Discovery in Asia: An Overview of E-Discovery and Asian Data Privacy Laws” (2015) 21 Rich JL & Tech 12.

However, exemptions from, and exceptions to specific Principles may apply.³⁴

a General Principle (individuals' consent and other legal grounds for legitimate processing) (section 6)

41 As a rule, the General Principle forbids a data user to process an individual's personal data without his or her consent. The Personal Data Protection Regulations specify that consent has to be "recorded" and "maintained", which implies that express consent is needed. It seems "implied consent" can be adequate, provided that the person/individual has been made completely aware of the goal regarding the processing of his personal data. The data user must be capable of illustrating that consent has been provided by the individual. Explicit consent is needed to process "sensitive personal data" such as data about religious beliefs, political opinion, health and commission or alleged commission of an offence.

42 A data user may process personal data about a data subject if the processing is necessary:

- (a) for the performance of a contract to which the data subject is a party;
- (b) for the taking of steps at the request of the data subject with a view to entering into a contract;
- (c) for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by a contract;
- (d) in order to protect the vital interests of the data subject;
- (e) for the administration of justice; or
- (f) for the exercise of any functions conferred on any person by or under any law.

34 The Personal Data Protection Act 2010 (Act 709) exempts certain activities from the scope of application of the Principles comprising of personal data processed for the detection or prevention of wrongdoing; the prosecution or apprehension of offenders; in connection with any court decision or order; the goals of investigations; or the purposes of removing regulatory roles if the utilisation of those provisions would be likely to be detrimental to the usual release of those regulatory roles.

43 In any case, personal data shall not be processed unless:

- (a) the personal data is processed for a lawful purpose directly related to an activity of the data user;
- (b) the processing of the personal data is necessary for or directly related to that purpose; and
- (c) the personal data is adequate but not excessive in relation to that purpose.

b Notice and Choice Principle (section 7)

44 A data user is to notify the individual by written notice, in both the national and English languages, of particular matters along with the fact that the personal data of the individual is being processed and a representation of the data; the aims behind the collection and further processing of the personal data; the individual's right to demand access to and amendment of the personal data, and the communication details of the data user in the event of any complaints or inquiries; the class of third parties to whom the data are or may be disclosed; any information accessible to the data user as to the origin of that personal data; and the means and options presented to the individual to restrain the processing of the data and whether it is voluntary or mandatory for the individual to supply data, and if mandatory, the outcomes of not complying.

45 The above notice must be delivered by the data user "as soon as practicable", meaning, meaning, when the data user first collects or asks for the personal data from the data subject, or before the data user applies the personal data for a purpose that is different from the primary purpose or discloses the personal data to a third party.

c Disclosure Principle (section 8)

46 This Principle forbids the disclosure of personal data, without the data subject's consent, for any purpose other than that for which the data was revealed at the time of collection, or a purpose related to it; and to any party other than a third party of the class originally specified to the data user.

d Security Principle (section 9)

47 The PDPA makes the data user liable for not taking measures to guard the personal data at the time of processing from any loss, modification, unlawful or accidental access or disclosure, misuse, alteration or destruction.

48 Where the data processing is managed by a third party (a “data processor”) in support of a data user, the data user needs to ensure that the data processor gives adequate guarantees in terms of the organisational and technical security standards governing the processing and takes reasonable measures to assure compliance with those standards.

49 Under the Personal Data Protection Regulations, data users are required to have a security policy abiding by any security standards issued, although no standards of any sort have been announced yet.

e Retention Principle (section 10)

50 As *per* this Principle, retention of personal data cannot be prolonged beyond what is required in order to satisfy the purpose for which they are processed. Further, a duty is imposed on the data user to take sensible measures to ensure that all personal data are destroyed or erased permanently if they are not needed anymore for the object for which they were processed.

f Data Integrity Principle (section 11)

51 The data user has to take sensible measures to ensure that the personal data are not misleading, correct, impeccable and kept up-to-date, with respect to the intent (and any direct relevant purpose) for which they were gathered and processed.

g Access Principle (section 12)

52 The PDPA provides the individual with the right to access and amend his own data wherever it is incomplete, misleading, inaccurate or outdated, except where under the PDPA the data user may decline to abide by a data correction or data access call by the individual.

iv *Rights of data subject (Part II, Division 4)*

53 Further to the right of access mentioned among the PDPA's "key principles", the following rights (subject to qualifications) are granted by the PDPA to individuals *vis-à-vis* a data user with respect to their personal data:

- (a) the right to access personal data;
- (b) the right to correct personal data;
- (c) the right to withdraw consent to process personal data;
- (d) the right to prevent processing likely to cause damage and distress; and
- (e) the right to prevent processing for direct marketing.

v *Registration of data users*

54 The PDPA provides that several categories of data users must be registered: banking and financial institutions, insurance, health, communications, education, direct selling, services, transportation, tourism and hospitalities, real estate and utilities, *etc.* There are chargeable fees for registration and the registration is valid for 24 months, after which renewal is needed.

55 Further, the Minister may ask for codes of practice to be issued, and data user forums to be established for data users who have to be registered.

vi *Offences and liability*

56 The PDPA has created several new criminal offences for the failure to comply with the provisions of the law. Some of the criminal offences are: (a) contravention of the Personal Data Protection Principles; (c) failure to register as a data user for specified classes of data users; (c) continuing to process personal data after revocation of the data user's registration; (d) unlawful collection or disclosure of personal data; (e) processing of personal data after a data subject withdraws consent; (f) failure to comply with the Commissioner's requirements to cease processing of personal data likely to cause damage or distress; and

(g) failure to comply with the Commissioner's requirements to cease processing of personal data for purposes of direct marketing.

vii *Enforcement mechanisms*

57 The Minister shall appoint any person as the Commissioner to enforce the law. The law empowers the Commissioner to investigate any possible breach on the part of a data user, upon a complaint from an individual or on his own initiative. When the Commissioner is of the opinion that a data user has contravened or is contravening a provision of the Act, the Commissioner may serve him with an enforcement notice.

58 In the enforcement notice, the Commissioner will state his opinion that the provision(s) of the PDPA has/have been contravened. The Commissioner will specify the provision(s) and the basis of his opinion. The Commissioner will direct the data user to take steps to rectify the breach within a specified period. The Commissioner may also direct the data user to cease the processing of the personal data pending the rectification of the contravention. The decision of the Commissioner on this issue and on other matters can be appealed to the Appeal Tribunal.

59 The different actors with relevant powers of enforcement under the PDPA are represented in Figure 1:

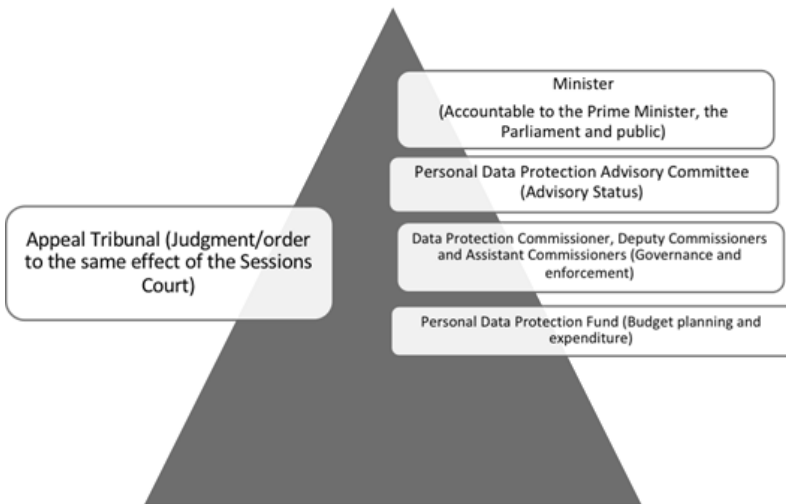


Figure 1

viii *International data transfers*

60 Again, similar to that of the European Data Protection Directive, specific requirements apply to the movement of data outside Malaysia under the PDPA. Data users can shift data to a place designated by the Minister of Culture, Information and Communications, or in application of one of the exclusions, *eg*, with the individual's approval or for the fulfilment of a contract.

**F TRANSFER OF PERSONAL DATA OUT OF MALAYSIA
(SECTION 129(1) OF PDPA)**

i *Current law*

61 Section 129(1) of the PDPA is the provision of the Act which regulates the transfer of personal data outside of Malaysia.

62 As a rule, this section provides that a data user shall not transfer any personal data to a place outside Malaysia, unless such place has been specified by the Minister, upon the recommendation of the Commissioner, by notification published in the *Gazette*.

63 In the absence of a published white list, data users in Malaysia must rely on one of the exemptions provided by section 129(3) of the PDPA in order to transfer personal data outside Malaysia. These exemptions include (among others):

- (a) where the data subject has consented to the transfer;
- (b) where the transfer is necessary for the performance of a contract between the data subject and the data user;
- (c) where the transfer is necessary to protect the vital interests of the data subject; and
- (d) where the data user has “taken all reasonable precautions and exercised all due diligence” to ensure that the personal data will not be processed in the recipient country in a way that would be a contravention of the PDPA.

ii “White List” for personal data exports

64 Whether a country qualifies to join the “white list” depends upon whether the Commissioner concludes that the country meets the criteria in section 129(2), namely that:

- (a) the country has a law which is “substantially similar to” the PDPA, or that “serves the same purposes” as the PDPA; or
- (b) the country otherwise ensures a level of protection in relation to the processing of personal data that is “at least equivalent to the level of protection afforded” by the PDPA.

65 In April 2017, the Commissioner issued a Public Consultation Paper (PCP) No 1/2017 entitled “Personal Data Protection (Transfer of Personal Data to Places Outside Malaysia) Order 2017” (“Consultation Paper”). The Consultation Paper seeks feedback from the public on the Commissioner’s long-awaited draft “white list” of countries to which personal data originating in Malaysia may be freely transferred. This marks an important step towards full implementation of the personal data export restriction in section 129(1) of the PDPA.

66 The Commissioner states in the Consultation Paper that he has considered the following in devising his draft white list:

- (a) countries that have comprehensive data protection laws in place (whether a single comprehensive data protection law or a combination of laws);
- (b) countries that have no comprehensive data protection law but are subjected to binding commitments (*eg*, multilateral/bilateral agreements); and
- (c) countries that have no data protection law but have a code of practice or national co-regulatory mechanisms in place.

67 If the Minister of Communication and Multimedia adopts the white list, as finalised by the Commissioner, data users will be able to freely transfer personal data to countries on the white list without relying on any particular exemptions. Personal data exported from the country will remain subject to the requirements of the PDPA, meaning that, for example, arrangements for secure processing offshore will still need to be put in place.

iii *Countries in draft white list*

68 The Commissioner's proposed white list is included in the draft Personal Data Protection (Transfer of Personal Data to Places outside Malaysia) Order 2017 ("Draft Order") as part of the Consultation Paper. The draft list is no doubt controversial and may in some cases be difficult to reconcile with the guiding logic for the list.

69 Perhaps unsurprisingly, the European Economic Area, the UK and jurisdictions that have been recognised by the European Commission as adequate for the purposes of European personal data exports are included on the list, comprising Andorra, Argentina, Canada, the Faeroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.

70 Regionally, Australia, China, Hong Kong, Japan, the Philippines, Singapore, South Korea and Taiwan have all been placed on the draft list. The US (not limited to the Privacy Shield framework) and the Dubai International Finance Centre have also been proposed. Despite the fact that China does not have a comprehensive law, apart from several provisions in the Cyber Security Law, the country is listed.

71 Notable omissions in the region include India and Macau. India's Information Technology Act 2000 is a form of relatively comprehensive data protection law, but pursuant to the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, the law is understood to not apply to the personal data of foreign data subjects sent to India for offshore processing. Macau's Personal Data Protection Act, on the other hand, dates back to 2005 and stands as one of the region's closest approximations to European data protection law.

72 The above list remains open to consultation and is subject to change. It may be that some of these countries will be removed from the list, and/or that other countries will be added to the list when the final Order is published. The deadline for providing feedback on the Consultation Paper was 4 May 2017.

73 Until the white list is finalised and published in the *Gazette*, data users must continue to rely on the exemptions provided in section 129(3) when transferring personal data outside Malaysia.

74 The upshot of the Commissioner's publication of the draft white list is that it may start a dialogue amongst lawmakers and regulators regionally on efforts towards interoperability of the region's increasingly dense thicket of cross-border data transfer restrictions and data localisation requirements. The Asia-Pacific Economic Cooperation ("APEC") Privacy Framework introduced in 2004 was put forward by regional economies as a common set of signposts towards the free flow of personal data across the region, with the intention that increased data protection regulation would be seen as complementary with, rather than antagonistic towards, free flows of personal data. This ambition has yet to be achieved, and given that the growth of advanced, high tech economies in the region is likely to be aided by moves towards interoperability, Malaysia's open commentary on the adequacy of other data protection laws in the region is a welcome step forward.

G DATA TRANSFER NEEDS AND EXPERIENCES OF COMPANIES BASED IN MALAYSIA

75 In this report, interviews with five companies based in Malaysia are summarised. The selected companies are of different sizes and from diverse economic sectors. While this selection does not represent all the companies which may be influenced by data protection law, it is still telling as it demonstrates that data transfers are crucial for business.

76 This summary will show how these companies all rely on data transfers, as data movements are intimately related to trade, and companies rely on shifting data as part of their global operations. The needs of the five interviewed companies can be sorted into two divisions; as part of processes within the company or company group and as part of their business offers. The former is about internal efficiency while the latter can be represented as growing external efficiency. The section goes on to discuss how data protection regulations affect their businesses.

i *Data transfer as part of business offer*

77 All the companies that were interviewed depend on digital means to market and deliver their products (goods or services). They use data transfers in three ways:

- (a) First of all, this involves the actual delivery of services (for instance, online services), but also consists of sending data of customers (which includes both private individuals (“B2C”) and B2B companies) and other marketing, online payments, billing, *etc.* Consequently, data movements between buyer and seller are essential to start and finish a transaction.

Subsequently, the continuation of relationships with their customers’ companies also uses data transfers, such as running and monitoring of the products (Internet of Things), examining the efficiency and identifying repair requirements or performing software upgrades. Also, this may be the outcome of consumers’ call for uninterrupted support (or access to the service) *per se*, data transfer requirements between seller and buyer are not a one-off transaction but are continuous.

- (b) Secondly, third-party digital services such as cloud solutions are used by some of the firms which are presented in this study, as part of the services given to the customers (*ie*, they use these services). In such instances, the companies are reliant upon the capability to receive and send data to and from (for example) the cloud provider. If this is not possible, the firms cannot provide their services to their customers.
- (c) Thirdly, several companies that were interviewed act as the supplier of a third-party digital service (*eg*, a cloud supplier) or provide digital infrastructure services (*eg*, telephone services), that is, they extend these services. These companies work as facilitators for others and rely on data transmission to ensure that other companies can provide their individual services. In such instances, a limitation on the capability to move data will, consequently, affect other companies’ abilities to deliver their services.

78 Another important point is that companies have put enormous effort into creating online solutions and transferring data efficiently. Identifying and employing the right third-party service provider is also a

focal concern for companies. Data is utilised to create universal value chains and to fragment production, enabling companies to specialise in particular assignments. In this case, data transfers are used to lower costs, secure efficient and smooth operations, and subsequently the capacity to remain competitive. A primary cause for the companies to transfer data is the capacity to centralise data processing in one location, which, as found during the interviews, is common in Malaysia. As data processing becomes more efficient and, subsequently, so does the business offer.

79 The data moved in all these cases incorporate both merchant and end customer data; nonetheless, a big part is also technical data – which include both non-personal and personal data.

ii *Data transfers for internal processes*

80 This study found that a portion of all the interviewed companies also use data transfers for internal operating. Data movements are perceived as essential to boost internal efficiency and to assure that the business set-up is equally effective and satisfies the requirements of the individual company.

81 The majority of the interviewed companies require the shifting of human resources (“HR”) data to and from headquarters. Another purpose of transferring data is to transmit them to research and development (“R&D”) facilities overseas to allow for product development. In fact, if companies were not able to transfer data, launching R&D units overseas would come at a higher expense, which would be even more problematic as some companies need to avail themselves of necessary skills which, in numerous instances, might not be available in Malaysia.

82 To increase efficiency, many companies utilise cloud solutions and data transfers. One reason brought forward by several interviewees was that cloud solutions enable prompt information gateways for all employees at any location, at any time. This is deemed to be significant for efficient work procedures, clarity, and, finally, competitiveness. For outsourcing processes, data movements are also necessary.

83 To get an effective outsourcing solution, the outsourcing partner must have an entrance to related data. This also combines both non-personal and personal data.

iii *Effect of data barriers on business models*

84 We will now focus on how data protection law can transform business models and trading opportunities. Based on the interviews, this part shows the viewpoints expressed by the companies.

85 The case studies emphasise that data protection laws have an impact on and are connected with many areas of the economy. Data protection thus cannot be labelled as just an ICT-only issue, and affects all sectors simultaneously. This is a focal point since the argument mostly focuses only on high-tech companies or on the impacts on big cloud providers. Nearly all companies make use of the Internet and if someone (or something) is connected to the Internet that indicates that data is likely to be distributed.

86 As a matter of fact, both small and medium-sized enterprises (“SMEs”) and low and medium-technology companies, too, are affected by the data regulations. The increase in efficiency for this big body of companies may similarly be influenced by data transfer limitations.

87 The interviewed representatives from all the companies are in favour of data protection, with a few even in favour of greater protection for individuals’ data. Although the focus of the interviews was on barriers, several companies came up with examples of how data protection laws make a positive impression on their businesses. One company even mentioned that restrictions on the processing of personal data have in fact guided them to examine what data they have accumulated and why (this particularly involved internal processes). In this fashion, personal data remain secure while internal processes are streamlined.

88 Finally, as a hard fact, several companies highlighted that Malaysia can use the demand for data storage as a trading point. Their customers feel protected knowing that the data were stored in their own jurisdiction, which in turn builds trust.

89 All the interviewed companies agreed that if there were no data flows, there would be no business. As all the business models are based on data transfers, trade would be impossible if data were not transferred in some part of the transaction. Some examples were given on how excessively restrictive data regulations have transformed trade – a major obstacle was how data regulations could frustrate business opportunities by causing delays and increasing costs.

90 Blockage on cross-border data streams further diminishes the capacity to match up to the most efficient services and technologies as the component of their business processes. The finest examples are restrictions that bar using cloud computing services, which are used to outsource both hardware and software, hence, improve efficiency and decrease costs. The localisation requirements are the most severe obstacles to the use of cloud computing, which definitely make the use of cloud computing difficult.

91 Laws relating to personal data can similarly function as an impediment to the use of cloud computing as shifts of entities outside Malaysia are restrained. Several companies raised the fact that these constraints on data transfer result in a situation where processing needs to be performed in different locations rather than in one prime location.

92 Investment decisions are similarly affected by data protection laws. Some companies who offer services to consumers emphasised the point that limitation while transferring personal data becomes an impediment since it makes it difficult for companies to classify customers.

93 In the interviews, companies stressed that restrictions on transferring data to third countries is a key business barrier. Malaysian data protection laws are comparatively stern policies in comparison to other countries. This entails a competitive disadvantage for Malaysian firms *vis-à-vis* their competitors in other countries (primarily Singapore, India and China, *etc*).

iv *Burden of compliance*

94 All regulation involves compliance concerns and data protection law is no exception. Nevertheless, the pressing questions are “what sort of compliance?” and “how does it influence business?”

95 There are two major categories of compliance costs: operational (*eg*, local storage) and administrative (*eg*, new routines and processes).³⁵ All companies stated that they put a lot of effort into ensuring compliance with data regulation while concentrating on the administrative costs. One company noted that both outside and within Malaysia, their main difficulty with data protection law is the time and administration required to evaluate and execute diverse legal variations. By embracing internal regulations that are built on the eminent standards, several companies have resolved the obstacle of differences in standards between countries.

96 Taking compliance further includes negotiating contracts to clarify data ownership and to ensure data protection. Similarly, ensuring compliance while using cloud services or outsourcing requires large amounts of money and time. Often, companies need to pay for external guidance to make compliance perfect, particularly when generating or rolling out new systems or services. While some firms take on compliance expenses without concern, others emphasise the expenses they incur. Building data systems in which individuals tick boxes to show the acceptance of handling of personal information is also expensive.

v *Companies want harmonisation of rules*

97 The need for harmonisation of data protection laws was an evident message that appeared from the interviews. Differences in legislations and legal interpretations within the region should be reduced in a co-ordinated manner. Each interviewed company ask for harmonisation with countries outside Malaysia.

35 *Human Resource Information Systems: Basics, Applications, and Future Directions.* (M J Kavanagh & R D Johnson eds) (Sage Publications, 2017).

98 Interviewees indicated how the differences in various jurisdictions bring about adoption expenses and even missed trade opportunities. One of the companies explained how the legislative variations hinder the provision of new services which it hopes to introduce simultaneously in all markets. Another company found that variations entail ambiguity and doubts as to sharing information, even within the company. Therefore, clearer rules and harmonisation would be highly useful for companies.³⁶ “Data protection cannot mean data protectionism” as Neelie Kroes, Vice-President of the European Commission, put it.³⁷

99 Regarding the variation in regulation within a territory, the interviewed companies are not asking for full harmonisation, instead the companies deem that the best solution would be to have high standards of protection in other countries – just high enough to be rated as corresponding with the EU/US standards and not so strict as is the case today.

vi Technology and secure data transfers

100 The law is not the only way to protect personal information and to secure safe data movements. A full-fledged communications infrastructure and technology are also essential tools to protect data; technology complements the law.³⁸

101 While handling data, safeguarding the integrity of the data and preventing leaks is crucial, not least for data processors. In this study, a number of companies highlighted the importance of developing systems with tight security to prevent breach of national data protection laws. This is also viewed as a competitive advantage, mainly when operating with clients in countries where worry about personal

36 P Lambert, *Understanding the New European Data Protection Rules* (CRC Press, 2017).

37 N Geppert, “Could the ‘EU-US Privacy Shield’ Despite the Serious Concerns Raised by European Institutions Act as a Role Model for Transborder Data Transfers to Third Countries?” *SSRN Electronic Journal* (January 2016).

38 *Communication Technology and Social Change: Theory and Implications* (C A Lin & D J Atkin eds) (Routledge, 2014).

information is relatively high. Furthermore, the companies highlighted as hard fact that an efficient way to make data less vulnerable and secure it at the same time is to disperse it geographically, meaning, for data storage to be in diverse countries. *De facto*, scattering data across numerous countries makes access flexible and improves security as owners/users of data are not under the control of one single country.

102 To ensure safe data movement and storage, very strong security systems have to be installed. Again, obviously, as costs increase it becomes a challenge. Prominently, numerous companies employ different levels of security as *per* their data requirements. Personal data are moved within systems with greater security than corporate or technical data. One company stated that running with a large international supplier raises the security of their clients. According to this company, to develop secure and compliant systems, compared to the smaller suppliers, these suppliers have more resources.

103 Additionally, security must be weighed against speed. Users must not experience delays in transfers, irrespective of their location in the world.

104 As such, speed is essential for the interviewed companies and their clients, especially since business models oftentimes demand instant access to information and data sharing without geography making a difference. Hence, for data transfers to be effective and for data to be secure, technology – particularly communications infrastructure – is essential. The infrastructure must allow for instant transfers of huge amounts of data as well as security measures.

H CONCLUSION

105 This study shows that business cannot take place if there is no movement of data from one place to another. Many services can become tradable and new service generation becomes possible due to the facilitation of the Internet and ICT solutions. This is doing business on a digital platform, that is, through transferring data. Moreover, machines, companies and people generate large amounts of data through the Internet. The application and movement of this data are a crucial part of businesses' daily transactions. Without data movement across the

borders, virtually no company from any sector can do business, much less think of taking part in international transactions.

106 In the interim, some data, particularly personal information, must be managed with caution. And for regulators, the lurking question is how they can achieve a proper symmetry between the protection of personal data and the need to transfer data.

107 The research here is not intended to approach the question of balance. The purpose is to illustrate how companies use data transfers in their business models and to trade. The purpose is to illustrate how companies can use data transfers in doing trade and in their business models. Moreover, the study demonstrates how laws restricting data transfer can influence business opportunities and operations. Based on the shown materials, this reporter would like to shed light on the subsequent important information the companies put forth when interviewed.

108 Predominantly, data and data transfers do not only concern big tech-savvy companies. In fact, they affect all companies. In order to run and be competitive, the low-tech sector SMEs rely upon data and data transfers more than anyone else. Intrinsically, data protection regulation must take into consideration the needs and requirements of an extensive array of companies.

109 Secondly, the law should be centred on specific sorts of data, not all data. Data localisation law, notably, is likely to include all kinds of data, which include completely technical data. To reduce business consequences, regulation has to converge as much as possible.

110 Thirdly, out of the two kinds of regulation, the companies are more concerned with the hostile outcome of forced localisation and similar regulation, which were discussed earlier in this report. Regulation of this sort is much more restrictive and, as *per* the companies, should be abolished. Regulation regarding the security of personal data is another aspect of relevance to ponder.

111 Finally, harmonisation is important for companies and removing variations in regulations between Malaysia and other countries would

promote trade. As a matter of fact, the larger the area where data can easily be moved, the lower the operating costs for companies.

Jurisdictional Report

NEW ZEALAND

Reporter: **Katrine Evans***
Senior Associate, Hayman Lawyers

A BACKGROUND INFORMATION

1 New Zealand is a small but well-developed economy which strongly recognises the importance of a free flow of personal information to facilitate both domestic and global trade. It also takes the view that, to facilitate that free flow of information, it is vital for economies to develop and maintain strong and effective privacy protection.

2 While New Zealand itself has comprehensive personal information protection legislation, in the form of the Privacy Act 1993, it accepts that privacy protection may take a variety of different regulatory forms (from overarching legislation to more self-regulatory models). There is an expectation that robust privacy protection will be based on a commonly agreed set of core privacy expectations, and supported by an effective system of enforcement and assurance.

3 A new Privacy Bill was introduced to the New Zealand Parliament on 20 March 2018. It substantially re-enacts the existing legislation but makes various changes to update the law. The timetable for passing the Bill is not yet clear and, of course, its final form may also change, but this report includes comments on the version of the Bill as introduced.

4 It is common for other domestic statutes to create specific rules relating to aspects of collection, handling and use of personal information in particular contexts (such as tax secrecy, or rules applying to intelligence

* The reporter gratefully acknowledges the contributions of the Office of the Privacy Commissioner of New Zealand to the responses to the original questionnaire on the basis of which this report was drafted. All errors are this reporter's own.

agencies, immigration or child protection). However, the Privacy Act is only overridden by those other laws if that is clearly Parliament's intention.

5 In addition to New Zealand's laws that apply to personal information, various policies have been developed over time that regulate or provide guidance to agencies that need or wish to engage in international data flows, or businesses that wish to offer services in that area. An example is the existing "Cloud First" policy that requires government agencies to prefer cloud services to traditional in-house IT where feasible.¹ This policy seeks to take advantage of the cost effectiveness, flexibility and greater choice afforded by cloud services (including offshore cloud), but is supported by fairly strict due diligence requirements for security and privacy.

6 New Zealand's approach to international data flows has been influenced by its long-standing and active membership of the Organisation for Economic Co-operation and Development ("OECD"). Its principal data protection legislation, the Privacy Act 1993, is expressly based on the OECD's 1980 "Guidelines for Transborder Flows of Personal Data". It is also an active participant in the creation of international privacy standards, including in the Asia-Pacific region. In particular, it has played a significant part in the development of the Asia-Pacific Economic Cooperation ("APEC") Privacy Framework and Cross-Border Privacy Rules system ("CBPR"). From 2014–2017, the New Zealand Privacy Commissioner was also the Secretariat for the International Privacy and Data Protection Commissioners' Conference.

7 The Privacy Act 1993 is an overarching statute whose principles apply equally to government agencies and private sector agencies, regardless of their size or financial means. It is one of the few data protection regimes outside Europe that has been recognised as "adequate" by the European Commission.

1 "Why Agencies Must Use Cloud Services" (ICT.govt.nz, Guidance and Resources).

8 Having adequacy status reduces the barriers and compliance costs that might otherwise exist for New Zealand businesses that handle or process personal information from a variety of jurisdictions.

B GENERAL LEGAL FRAMEWORK OF INTERNATIONAL TRANSFERS OF PERSONAL INFORMATION

i *Existing data privacy protections in national legislation*

9 New Zealand has comprehensive legislation on the protection of personal information: the Privacy Act 1993.

10 The Privacy Commissioner has also issued several codes of practice under the Privacy Act, which become part of the law and which modify the privacy principles in relation to specific industries. The main Codes are the Health Information Privacy Code 1994, the Credit Reporting Privacy Code 2004 and the Telecommunications Information Privacy Code 2003.² There are no specific provisions relating to cross-border transfers in the Codes, but the Codes may govern transactions with a cross-border element. For example, call centres providing services on behalf of external clients are agencies that have to comply with the Telecommunications Information Privacy Code.

11 Complaints about breaches of the Privacy Act are investigated in the first instance by the Privacy Commissioner. If the dispute is not resolved by the Commissioner, a specialist tribunal exists to hear cases alleging breaches of the privacy principles or Codes. This tribunal is the Human Rights Review Tribunal, which is established under part 4 of the Human Rights Act 1993.

12 The provisions in the Privacy Act that are most obviously applicable to cross-border transfers of personal information are:

- (a) Section 10: Personal information is still legally “held” by a New Zealand agency if it is transferred out of New Zealand by that agency or another agency (for example when using an offshore cloud service provider). This means that the New Zealand

2 Office of the Privacy Commissioner, “Codes of Practice” (Privacy Act and codes).

agency is still responsible for the security, accuracy, retention, use and disclosure of that information. The New Zealand agency is also still responsible for providing access to the information on request from the individual concerned and responding to any requests by the individual to correct it.

- (b) Part 11A deals with the ability of the Commissioner to prohibit a transfer of personal information to another State where that personal information has originally been sent to New Zealand from another jurisdiction and the receiving jurisdiction does not have comparable privacy safeguards to our own. It specifies the contents and conditions of issuing a transfer prohibition notice, creates an offence for a failure to comply with a transfer prohibition notice and sets out a right of appeal.

13 A new Privacy Bill was introduced to the New Zealand Parliament on 20 March 2018. It reflects all the key features of the existing Privacy Act (including the information privacy principles, and the functions of the Privacy Commissioner). However, it also includes new provisions that will implement many recommendations of the New Zealand Law Commission's review of the Privacy Act, which was published in 2011.

14 Among other amendments (such as mandatory breach notification requirements), the Bill contains some new provisions on cross-border transfers of personal information. It will address the existing lack of clarity about protection of personal information that originates in New Zealand (rather than being transferred here from another State), and that is then sent offshore.

15 In particular, a new clause has been added to principle 11 (the privacy principle governing disclosure).

16 Principle 11(3) states that an agency ("A") may not disclose personal information to an overseas person ("B") who is not subject to the Privacy Act unless:

- (a) B is acting as an agent for A, in relation to safe custody or processing of personal information (that is, there is a principal agency that is legally liable for the information under New Zealand law); or
- (b) the individual authorises the disclosure of the information; or

- (c) B is in a “prescribed country or State”; or
- (d) A believes on reasonable grounds that B is required to protect the information in a way that, overall, provides comparable safeguards to those contained in the Privacy Act (one example is where A and B have an agreement that provides for those safeguards: principle 11(5)); or
- (e) the disclosure is to the individual concerned; or
- (f) the source of the information is a publicly available publication and it would not be unfair or unreasonable to disclose the information in the circumstances.

17 Principle 11(4) adds that it is also acceptable to disclose the information if A reasonably believes the disclosure is necessary for safety purposes, law enforcement, court proceedings, protection of public revenue, or enforcement of a law with a pecuniary penalty, and it is not reasonably practicable to comply with the requirements of principle 11(3).

18 A “prescribed country or State” is one that is specified in regulations as having privacy laws comparable to those of New Zealand (principle 11(6)). The Ministry of Justice will be responsible for developing those regulations. It will be important for the content of those regulations to be signalled well in advance of the commencement of the new legislation, so that businesses have time to analyse their existing contracts and adjust their arrangements with overseas organisations if necessary.

19 A variety of other statutes make provision for receiving or transferring personal information across borders, or controls over what can be received or transferred, in particular situations. Examples include the Mutual Assistance in Criminal Matters Act (which supports cross-border information gathering for the purposes of criminal investigations, within specified limits), border control legislation such as the Immigration Act 2009 or the Customs and Excise Act 1996, schemes for mutual recognition of pensions under the Social Welfare (Reciprocity Agreements) Act, and the Intelligence and Security Act 2017 that governs our intelligence and security agencies (for instance section 14, which allows the intelligence agencies to co-operate with others, including overseas agencies, to respond to an imminent threat).

20 New Zealand's constitution is based on the Westminster system of government and is largely unwritten. There is no specific reference to privacy or data protection in the small number of constitutional statutes that we do have (such as the Constitution Act 1986, and the New Zealand Bill of Rights Act 1990), though there are protections for privacy-related issues such as protection against unreasonable search and seizure (section 21 of the New Zealand Bill of Rights Act).

21 The courts have also recognised a civil action for breach of privacy, as part of the law of tort. This development relied in part on a view that privacy was an existing right in New Zealand that, while not expressly recognised in the New Zealand Bill of Rights Act, could act as a justifiable limitation on other rights.

22 Few data protection cases reach the ordinary courts, as they are predominantly dealt with by the specialist tribunal (the Human Rights Review Tribunal) which was established to hear cases under the Privacy Act. However, occasionally, cases with data protection angles do reach the courts.

ii *International engagement*

23 New Zealand ratified the International Covenant on Civil and Political Rights ("ICCPR") on 28 December 1978, with certain reservations. It ratified the first Optional Protocol to the International Covenant on Civil and Political Rights on 26 May 1989, and the second Optional Protocol (referring to the abolition of the death penalty) on 22 February 1990.

24 The Ministry of Justice is responsible for administering the ICCPR and the Optional Protocols.

25 New Zealand has signed a variety of free trade agreements (for instance with Singapore, China and Korea),³ and some provisions may, at

3 See <<https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/>> (accessed 9 April 2018).

least indirectly, either maintain or affect privacy protection though their effect has not been fully tested as yet.

26 New Zealand signed the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (“CPTPP”) on 8 March 2018, though the Agreement has not yet been considered by Parliament and is therefore not in force.⁴ The Electronic Commerce chapter of that Agreement (in Article 14.8) contains provisions that require signatories to have or develop legal frameworks to protect personal information, which take into account principles and guidelines of relevant international bodies. Article 14.8(5) acknowledges that the types of legal approaches may differ between jurisdictions, but the effect of it is that “each party should encourage the development of mechanisms to promote compatibility between these different regimes”.⁵

27 New Zealand is an APEC Member economy, and participates in the APEC Cross-border Privacy Enforcement Arrangement (“CPEA”). It has not yet joined or lodged a Notice of Intent to participate in the APEC CBPR system. Any decision about joining the scheme would be for the New Zealand government to make.

28 New Zealand is not currently an observer on the Consultative Committee of Council of Europe Convention 108. However, it has recently applied to become an observer and is waiting for a decision.

29 In December 2012, New Zealand was recognised by the European Union as offering an adequate level of protection in application of Article 25(6) of Directive 95/46/EC. In 2017, The European Commission has announced that it was reviewing the 12 adequacy decisions which it has with countries outside the bloc, including New

4 See <<https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/cptpp/cptpp-overview/>> (accessed 9 April 2018).

5 Blair Stewart, “What’s Happening with the Trans-Pacific Partnership” (Office of the Privacy Commissioner, 15 December 2017).

Zealand.⁶ As the Privacy Commissioner has stressed in his recent briefing to the new Justice Minister, it is becoming urgent that New Zealand should update the Privacy Act in order to ensure that it continues to meet that adequacy standard,⁷ since⁸

... as the European Commission has commented, adequacy decisions are living documents that it will regularly monitor, providing an adequate level of protection is an ongoing process and continued adequacy is not guaranteed. Each 'adequate' jurisdiction is expected not only to maintain the strength of its law, but also to update that law as required to meet the standards that Europe views as appropriate in our changing information environment.

The provisions of the new Privacy Bill will help to meet that aim.

30 New Zealand organisations that do business with Europe are likely to have to pay close attention to the effects of the European General Data Protection Regulation ("GDPR"). While New Zealand has adequacy status (see above), some new aspects of the GDPR go beyond what is in our existing laws. Examples include mandatory breach notification (notification in New Zealand is currently only voluntary), data portability and stronger enforcement (in particular New Zealand does not have any fines for breaches of the Privacy Act).

31 The Privacy Commissioner has recommended that the proposed new privacy legislation should include some of these key features, in order to maintain equivalent levels of protection to those available in the GDPR.⁹

6 Communication from the Commission to the European Parliament and the Council, "Exchanging and Protecting Personal Data in a Globalised World" (Brussels, 10 January 2017).

7 Office of the Privacy Commissioner, "Briefing for the Incoming Minister of Justice: Hon Andrew Little" (October 2017).

8 Blair Stewart, "Providing an Adequate Level of Data Protection: An Ongoing Process" (Office of the Privacy Commissioner, 27 January 2017).

9 Office of the Privacy Commissioner, "Privacy Commissioner's Report to the Minister of Justice under Section 26 of the Privacy Act" (Reports to Parliament and Government).

32 The version of the Privacy Bill that has been introduced to Parliament does not include some of the additional features that the Privacy Commissioner has recommended. For instance, it does not include prohibitions on re-identification of individuals from de-identified datasets, data portability, or accountability requirements.

33 However, amendments to the legislation are possible during its passage through Parliament, and there are likely to be strong submissions to the Select Committee on some of the Commissioner's recommendations.

34 Alternatively, even if the legislation remains unchanged, it may be possible to meet the same policy goals through a process of legislative interpretation. Most importantly, the Bill gives the Privacy Commissioner a new power to order agencies to amend their processes to comply with the law. A compliance order will have legal force. Agencies that fail to develop sound policies and frameworks to ensure compliance are much more at risk of being subject to a compliance order. While this falls short of being a direct obligation on the agency to be able to demonstrate accountability, it may be capable of achieving a similar aim.

iii Role of Office of the Privacy Commissioner of New Zealand in the area of cross-border data flows

35 The Privacy Commissioner, established under the Privacy Act 1993, is a statutory authority that is publicly funded but independent of government control. Among the Commissioner's functions is application of the Privacy Act's rules on international transfers of personal information.

36 The Privacy Commissioner is the only authority that administers the Privacy Act. However, other agencies provide enforcement in related areas of practice, which in some countries are enforced by the data protection authorities. For instance, the Department of Internal Affairs has responsibility for administering the legislation relating to unsolicited electronic messages (spam).

37 The Privacy Commissioner has the ability to prohibit cross-border transfers of personal information under certain circumstances: see part 11A of the Privacy Act, as discussed above.

38 The Privacy Commissioner has produced a Fact Sheet on the transfer of personal information outside New Zealand.¹⁰ The Fact Sheet explains the process that the Commissioner would follow, and the criteria that would apply to a decision to prohibit transfer of personal information. The Commissioner has not yet issued any transfer prohibition notices.

39 The Privacy Commissioner is an Accredited Member of the International Conference of Data Protection and Privacy Commissioners. The Office served as Secretariat for the Conference from 2014–2017 and the Commissioner chaired the Conference during that time.

40 There is no sectoral authority that enforces information transfer restrictions in the jurisdiction.

C DEFAULT POSITION, SCOPE AND TERRITORIAL EFFECT

41 The default position in the current law as to international transfers of personal information is that international transfers are permitted, as long as the legal requirements in the privacy principles and appropriate conditions for privacy protection are observed. Notably, the default position under the Privacy Bill will be that international transfers will not be permitted unless one of the acceptable conditions applies. Those conditions (listed above) are designed to ensure that the information is properly protected when sent offshore. They are unlikely to create a significant change in practice for those agencies that already perform due diligence for personal information protection, and that have sufficiently strong contracts in place.

42 All agencies that have a place of business and hold information in New Zealand are required to comply with the Privacy Act. Agencies that are based in New Zealand but hold all or some personal information offshore are also required to comply with the Privacy Act.

10 Office of the Privacy Commissioner, “Fact Sheet on Part 11A of the Privacy Act 1993: Transfer of Personal Information Outside New Zealand” (Guidance Resources).

43 The principles of the Privacy Act apply to all organisations in the private sector (as well as all organisations in government) regardless of their size or turnover, or the industry in which they operate.

44 The Privacy Act also applies to individuals, except in relation to their personal or domestic affairs. However, if a person acts in a way that can cause serious harm to others, the “personal or domestic affairs” exception will not apply: that is, the person can be in breach of the Privacy Act in the same way as other agencies may be.

45 New Zealand privacy law does not define certain categories of personal information as “sensitive”, and the privacy principles theoretically apply equally to all information.

46 In practice, the application of some of the privacy principles will vary depending on the nature of the information, as the context may determine what it is reasonable to expect of an agency (for example, the more harm an individual may suffer from a failure to keep information safe, the more steps it will be reasonable for an agency to take to protect that information against loss or misuse).

47 Similarly, the nature of the information is likely to be a factor that influences whether the Privacy Commissioner would issue a transfer prohibition notice (see the Fact Sheet mentioned earlier: a notice will be issued when it is proportionate in the circumstances to do so, and the level of potential harm to individuals is one factor that influences that calculation).

48 The Privacy Act does not use the terminology “data controller” or “data processor”: instead it refers to “agencies” that collect or hold “personal information”. There is only a small list of bodies or persons that are excluded from the definition of “agency” (see section 2 of the Privacy Act).

49 However, it is worth noting that:

- (a) Section 3(4) states that an agency that holds personal information solely as the agent for another, or for the purposes of safe custody, or for the purposes of processing is not itself responsible for the information as long as it does not use or

- disclose the information for its own purposes. Responsibility for privacy remains with the principal agency (that is, the body that has engaged the entity to hold or process the information on its behalf).
- (b) Similarly, section 10 states that agencies that hold information outside New Zealand remain liable for that information. The most obvious application of this provision is in the area of cloud computing.¹¹
 - (c) Section 10(3) specifies, though, that an agency holding information outside New Zealand does not breach the privacy principles if it is required to take action to comply with the law of another jurisdiction. This provision attempts to strike a balance between maintaining the application of New Zealand law to New Zealand-governed agencies, and recognising that those agencies also have to comply with the laws of the other jurisdictions in which they operate (which may not always be the same as, or compatible with New Zealand law). The question of whether personal information will be properly protected in those overseas jurisdictions therefore becomes important. If there is insufficient protection available for personal information, then this may serve to trigger a transfer prohibition notice if the personal information was originally sent to New Zealand from elsewhere (to be extended to information sourced from New Zealand under the proposed new privacy law once it is developed).

50 There are very few types of people or bodies that do not have to comply with the privacy principles. These are all listed in the definition of “agency” in section 2 of the Privacy Act. The only exceptions are: the Sovereign and the Governor-General; Parliament and Members of Parliament (“MPs”) acting in their official capacity (also Parliamentary Services, that provides support to the MPs and Parliament); courts and

11 See cl 20 of the Privacy Bill, and the additional clarification in cl 8 (which replaces s 3(4)). Clause 8 currently does not reflect the requirement in s 3(4) that the third party must hold personal information *solely* as agent, for safe custody or for processing. The omission of the word “solely” may reduce the protection afforded by the clause.

tribunals to the extent that the action relates to their judicial functions; Royal Commissions, and commissions of inquiry appointed pursuant to statute; the news media when engaging in news activities; and the Ombudsman. Of those bodies, only the news media operate in the private sector.

51 The law applies equally to information about individuals whose information has been imported into the country by a New Zealand entity. For example, foreign nationals have a right to access information about themselves that is held by a New Zealand agency, regardless of whether the foreign national is in New Zealand or elsewhere. This was an important change that had to be made to New Zealand law in order to gain adequacy.¹²

52 Agencies are required to take reasonable steps to protect personal information in transit as well as at rest (for example, by encryption).

53 Encrypted information is still classed as “personal information” under the Privacy Act (that is, “information about an identifiable individual”). However, anonymised information may, in certain situations, not be “personal information” – it will depend on whether the individual is realistically able to be re-identified (for example, by comparison with other information sources in the agency’s possession or available from public records).

54 The Privacy Act specifically permits use or disclosure of information as long as it has been anonymised, and permits uses or disclosures of information for research or statistical purposes as long as the results of the research or analysis cannot reasonably be expected to identify the individual (see for instance principle 11(h)). Collection from people other than the individual concerned is also permitted in the same circumstances.

55 However, the increasing ability to re-identify individuals, or to make assumptions or decisions in relation to individuals based on supposedly anonymised information, means that further protections are

12 Privacy (Cross-border Information) Amendment Act 2010.

required. The Privacy Commissioner has therefore recommended that there should be provisions prohibiting re-identification. The Law Commission also proposed that a new provision should be introduced requiring agencies to allow individuals to transact anonymously or pseudonymously, as long as the nature of the transaction permitted this. The previous government accepted that this should form part of the proposed new legislation.

56 Notably, though, the Privacy Bill does not currently contain a prohibition on re-identifying individuals, and does not reflect the Law Commission's recommendation on anonymous or pseudonymous transactions. The latter, in particular, is a significant and surprising omission and it is hoped that it can be addressed at the Select Committee stage.

57 The Privacy Commissioner has not published specific guidance on the interpretation of anonymised or pseudonymised information. However, he issued an Advisory Opinion in January 2017 that concluded that address information published on a website would be "personal information".¹³ This is useful guidance that illustrates that supposedly anonymised information may not, in practice, be anonymised at all.¹⁴

D LEGAL BASIS

58 The individual's consent is not always necessary to transfer their information under New Zealand law, although the agency needs to provide clear information about the transfer.

59 Other legal provisions apart from consent can allow a transfer to happen. The principal one is that transfer is one of the purposes of obtaining the information, or is directly related to one of those purposes. For instance, if transfer of the information is an unavoidable feature of a

13 Office of the Privacy Commissioner, "Privacy Commissioner's Report to the Minister of Justice under Section 26 of the Privacy Act" (Reports to Parliament and Government).

14 See John Edwards's keynote address at the 2015 Identity Conference, "Enabling Digital Identity and Privacy in a Connected World?".

business transaction (such as to enable performance of a contract), then it is likely that the transfer will be permitted on the basis that it is one of the purposes for which the information was obtained. However, it is important to note that the agency must still provide the safeguards set out in the other privacy principles, including the limitations on use and retention, and the requirement to take reasonable steps to make sure that the information is secure.

60 It is unclear whether there is any specific research on the level to which individuals in New Zealand object to offshore transfers of their personal information. There is a high level of mistrust about businesses sharing information without permission:¹⁵ 78% of respondents reported being concerned or very concerned. It is possible that concerns about offshoring may play a part in this high level of concern, but there is no firm evidence to that effect.

61 However, a survey from May 2011 by the Privacy Commissioner¹⁶ suggests that, at that time, information provided to individuals was not consistent. Some agencies in the survey stated that they had express consent for the transfer (though this would often have been in the form of standard terms and conditions, and individuals might not have been specifically aware of the contents). Other agencies did not inform individuals that their information might be sent offshore. The survey conclusion was that individuals will often be unaware that their information might be exported; the result is that they would have no real chance to object.

62 There is also little specific evidence about whether people change their behaviour as a result of any concerns that they have about offshoring of information. However, it is possible that behaviour would follow the patterns reported in the February 2015 report from Victoria University of Wellington's School of Government "Kiwis Managing Their Online Identity Information". That report suggests that most New

15 See the "Privacy Concerns and Sharing Data" survey commissioned by the Office of the Privacy Commissioner and conducted by UMR Research from 30 March to 18 April 2016.

16 Office of Privacy Commissioner, "Offshore ICT –New Survey Results" (Media Release 1 May 2011).

Zealanders are privacy pragmatists when it comes to managing their online identity, adjusting their behaviour to fit the context in which they are operating. Trust in the individual agency (such as a global company) will affect their willingness to engage. The report also highlighted that some people are fatalists about their privacy: they may engage anyway because they believe that they have no choice about what to do.

63 International transfers of personal information are not subject to a requirement of notification to, or approval by the regulator, government or public entity. The same will be true under the new Bill: the responsibility for legal compliance lies with the agency, and the Commissioner can intervene if the transfer appears to breach the law.

64 However, where government agencies wish to adopt cloud computing services, they must complete the due diligence requirements for security and privacy set out by the Government Chief Information Officer.¹⁷ Agencies are not allowed to place government data above a “Restricted” classification in any public cloud, whether onshore or offshore.

65 A variety of other statutes may provide a basis for international transfers of personal information, such as arrangements for information sharing between domestic and foreign government agencies.¹⁸

E DATA LOCALISATION

66 There is only one existing specific data localisation requirement in New Zealand, though agencies that propose to transfer information offshore may in practice be required to take some additional measures to ensure that they continue to comply with the privacy principles.

17 “Cloud Computing –Mitigating Risk” (ICT.govt.nz, Guidance and Resources).

18 For instance, the Trans-Tasman Mutual Recognition Act 1997 contains provisions dealing with mutual recognition of occupations between New Zealand and Australia, which imply the transfer of data of Kiwis to Australian public authorities. The Privacy Commissioner of the time issued a Report to the Minister of Justice on the impact of the resulting transborder data flows to Australian public agencies and concluded that he had no objection to the transborder data flow aspect of the Bill, given the protections in place in the Act.

67 The exception is that under the Tax Administration Act 1994 and the Goods and Services Tax Act 1985, tax information is required to be kept in New Zealand unless the Commissioner of Inland Revenue authorises its transfer offshore if the storage of those records offshore does not impede the Commissioner's compliance activities.¹⁹ Several commonly used services that offshore accountancy and tax information have been approved by the Commissioner of Inland Revenue.²⁰

68 As mentioned earlier, government agencies are not allowed to store information in a public cloud that is above "Restricted" classification, but this is equally true whether the public cloud is onshore or offshore.

69 The new Privacy Bill will effectively provide for greater localisation. It prohibits transfers of information offshore unless one of a variety of conditions applies to protect that information. However, it should still be relatively straightforward for agencies that perform effective due diligence (or that obtain informed consent) to send information offshore.

70 The restrictions in the tax legislation mentioned above apply whether information is held in physical or electronic form. Agencies that hold information offshore (with approval) still need to make sure that the information is available in a usable format, on request from Inland Revenue, and with no charge.

71 The Contract and Commercial Law Act 2017 generally permits information to be held in electronic format and for that information to be equally legally valid as original physical copies. There are few pieces of legislation that require retention of physical records. The Contract and Commercial Law Act also requires agencies to be able to fulfil their legal obligations to produce information, or to ensure that it is accessible in

19 Inland Revenue Standard Practice Statement, "SPS 13/01: Retention of Business Records in Electronic Format, Application to Store Records Offshore and Application to Keep Records in Maori" *Tax Information Bulletin* Vol 25, No 3 (April 2013).

20 Inland Revenue, "Third Party Providers Approved to Store Taxpayer Electronic Records Offshore" <<http://www.ird.govt.nz/technical-tax/general-articles/third-party-providers-e-records.html>> (accessed 9 April 2018).

response to a lawful request.²¹ This obligation will apply whether information is held onshore or offshore. It is therefore important for agencies to make sure that they can meet those obligations wherever in the world the information is held.

72 In relation to the tax legislation mentioned above, third-party companies (that is, companies that may offer services for holding or processing tax information offshore) can apply to the Commissioner of Inland Revenue for authorisation to store tax information offshore.

73 One relevant consideration for the Commissioner is “whether the third party carries on business in, or through, an establishment in New Zealand; and the procedure that the third party has for dealing with client data should the third party no longer hold records for the client”.²²

74 This requirement will only apply to information that is within the definitions of New Zealand’s tax statutes and within the Commissioner of Inland Revenue’s control. It will not apply to all information held by those third-party providers, for clients in other jurisdictions.

75 Current localisation requirements apply only to tax information, but they apply regardless of whether the taxpayer is an individual, a government agency or a private sector agency.

76 While there are few existing localisation requirements, the Privacy Commissioner can also issue transfer prohibition notices in certain circumstances (discussed above). In such instances, the nature of the information – and particularly the level of harm that an individual might suffer as a result of the transfer – may affect the Commissioner’s decision about issuing a notice.

21 See ss 233 and 235 of the Contract and Commercial Law Act 2017.

22 See para 11 of Inland Revenue Standard Practice Statement, “SPS 13/01: Retention of Business Records in Electronic Format, Application to Store Records Offshore and Application to Keep Records in Maori” *Tax Information Bulletin* Vol 25, No 3 (April 2013).

77 The Commissioner of Inland Revenue may grant an authorisation as discussed above. The authorisations already granted are listed (referred to above).

78 The localisation requirements apply whether or not the information has been encrypted.

79 The information provided by the Commissioner of Inland Revenue on the need for authorisation before offshoring tax information is firm. However, it is unclear whether, in practice, Inland Revenue takes any steps to identify and enforce the provisions requiring authorisation.

80 Any company wishing to offer services for storing and processing tax information offshore would be well advised to seek authorisation: the chances of being investigated are reasonable. The principal providers in New Zealand appear to have done so.

81 However, it is unlikely that all individuals or agencies would be aware of the rule or would check that any company that they are using to store their tax information offshore has received appropriate authorisation.

F DATA TRANSFER MECHANISMS

i *Preliminary issues*

82 Different jurisdictions, cultures and legal systems often need to construct their privacy protection in different ways. One size – or one type of privacy law – does not suit all – and privacy itself is culturally relative. It is therefore a fact of life that we will have multiple cross-border data transfer systems. Allowing jurisdictions to retain a sense of their own identity whilst still protecting privacy is highly beneficial. In contrast, imposing external restrictions that jar with people's norms, or with a nation's existing regulatory structures, seems likely to fail.

83 The more varied the transfer mechanisms are, however, the more this increases the costs and complexity of doing business in the region. It is hard to get a clear picture of what is required when laws and regulatory bodies differ significantly from country to country. Developing a set of understood and effectively implemented norms – and creating assurance mechanisms to ensure they are observed – is vital for success.

84 There is also an increasing need for cross-border enforcement – there is little point developing rules that cannot be enforced, as they will simply be ignored. It is therefore important to ensure that authorities can co-operate with one another. Providing a framework within which co-operation can occur is an important aspect of data transfer systems.

85 There is no hard information on the point, but the most frequent data transfer mechanism in New Zealand is likely to be contract (both consumer contracts and commercial contracts).

86 There is a significant burden involved with writing contracts (or deciding whether to accept contracts prepared by others) when operating across borders. Interoperability of laws reduces the level of costs and complexity involved.

87 Importantly, interoperability also increases the likelihood that personal privacy will be more effectively protected: the more divergence there is in laws and regulatory systems, the more likely it is that at some stage in the transaction, personal information will be compromised in unacceptable ways.

88 While the New Zealand government has not been particularly active in this space, the Office of the Privacy Commissioner has been significantly involved in the development of the APEC Privacy Framework, CPEA and the CPBR scheme.

89 At the moment, there is no threshold legal obligation to ensure that the recipient is bound by legally enforceable obligations regarding the protection of the transferred information. For material that enters New Zealand and is then sent elsewhere, the possibility of a transfer prohibition notice should encourage exporters to check that the receiving jurisdiction has comparable protection available. For material that originates in New Zealand, the agency may not be able to fulfil its own legal obligations if it has failed to check that the receiving jurisdiction provides protection. The proposed new legislation sets out further obligations for exporters of personal information to observe (discussed above).

90 As long as the New Zealand agency that exports the data still “holds” the information (that is, it retains the ability to control it), the

New Zealand agency is still liable in case of a breach by the data importer. Contracts suggesting otherwise may have little force – at best they are likely to create an underwriting arrangement between the contracting parties.

91 If the New Zealand agency has divested itself of control altogether (for example by selling its business to the overseas data importer with all the associated customer information), it will have to justify that action under the privacy principles. Failure to do so, though, simply means the New Zealand agency is liable for compensation or other remedies for harm. The information that is with the data importer will not still be governed by New Zealand legal requirements.

92 New Zealand generally does not take a self-regulatory approach to privacy law. There are some exceptions – for example the print media are not covered by the Privacy Act, but the Press Council has developed industry self-regulation to deal with privacy issues (as well as other media standards such as accuracy and balance).²³

93 There is some level of self-certification in relation to privacy standards in the government sector, but those systems are subservient to the Privacy Act's requirements. In particular, all government agencies (with only very limited exceptions, such as Parliament) are governed by the legal obligations under the Privacy Act. However, they are also expected to self-assess their levels of privacy maturity on an annual basis, against the "Privacy Maturity Assessment Framework" developed by the Government Chief Privacy Officer.²⁴ Each agency is supposed to engage in a programme of continuous self-improvement against the measures set out in the Framework.

94 In areas other than privacy protection, New Zealand has a strong focus on statutory regulation, but also engages co-regulatory and self-regulatory mechanisms in certain industries, depending on the context and the benefits of legislative enforcement. An example is the Banking

23 New Zealand Press Council, "Statement of Principles".

24 "Using the Privacy Maturity Assessment Framework" (ICT.govt.nz, Guidance and Resources).

Ombudsman Scheme. New Zealand has strong statutory financial regulation, but the banks have established a code of practice and a self-regulatory consumer dispute resolution system to ensure that disputes can be settled easily and inexpensively without the need to take court action.

ii *“Adequacy findings” and white lists*

95 There is no general requirement in existing New Zealand privacy law that information can only be exported to countries with “adequate” privacy laws or that are on a white list.

96 However, the Privacy Commissioner can issue a transfer prohibition notice under section 114B of the Privacy Act, if the information has been sent to New Zealand and the jurisdiction to which the information is then to be exported does not have “comparable safeguards” to those provided in New Zealand law.

97 There is no formal process for recognising that the receiving jurisdiction meets standards of comparability at present. Under the proposed new privacy law (see above), regulations can be developed to define jurisdictions that have comparable privacy protections to those that apply in New Zealand (“white lists”). It is not clear if a principle of reciprocity or mutual recognition would apply.

98 It is not yet plain what criteria might be used under the new law to judge whether a receiving country’s law is acceptable, though it is likely that any jurisdiction covered by the GDPR, or with adequacy under the GDPR should automatically meet the correct standard.

99 The New Zealand Privacy Act itself was based on the OECD “Guidelines on Transborder Flows of Personal Data”, so this would be likely to be a relevant (though not necessarily a determinative) factor. Similarly, it is likely that another consideration would be whether the jurisdiction is a member of the CBPR and CPEA arrangements. Since application can vary between jurisdictions, further enquiry would be needed but membership would at least be a good start.

100 If the Privacy Shield arrangement stands the test of time, it may also prove to be a useful factor in considering whether individual data transfers to Privacy Shield participants are acceptable.

101 Whether the law could accommodate decisions of “sectoral adequacy” will depend on the shape of the new law, once passed.

102 Most of the discussion has focused on establishing white lists. There is no suggestion in the current version of the Privacy Bill that regulations could establish black lists. The issue may come up during the parliamentary process but the effort involved in developing blacklists might be too considerable to be worthwhile. Once the new provisions restricting export of personal information come into force, informal advice from the Privacy Commissioner might serve just as well if it ever proved necessary to warn against transfers to a particular jurisdiction. It would be harder for an agency to claim that it had sufficiently protected the information, or obtained properly informed consent, if it chose to transfer the information to a jurisdiction about which the Privacy Commissioner had expressed concern.

103 There is a limited discussion of different options and costs and benefits in the Ministry of Justice’s “Regulatory Impact Statement 1993: review of the Privacy Act” on the Ministry’s website (2012). For instance, the Ministry calculated that white lists could help to mitigate compliance costs for business. However, it recognised that doing due diligence on the privacy standards of additional jurisdictions is time consuming.

104 At that time it was anticipated that the Privacy Commissioner would compile the white list, and there was a suggestion that he might require an extra full-time equivalent for at least two years to complete the task. Now the Bill states that any white list will be set out in regulations, so the Ministry of Justice will be responsible for developing those regulations. The same resource problems arise. It will be important for the Ministry to allocate sufficient resources to the task.

105 The most likely immediate response will probably be to pass regulations acknowledging that European Union members that are covered by the GDPR, and third countries that have adequacy status under the GDPR are jurisdictions with sufficiently comparable

protections. The status of other countries can then be determined with more in-depth analysis. Some degree of urgency will be required, however, particularly with New Zealand's principal trading partners, including those with whom we have free trade agreements.

iii *Consent as exception to existence of privacy safeguards overseas*

106 Consent would not currently appear to waive the requirement of existing privacy safeguards in the country of destination. The legislation does not mention it, nor does the Privacy Commissioner's Fact Sheet on transfer prohibition notices.²⁵

107 Under the new Bill, principle 11(3)(b) states that an agency can disclose personal information to an overseas person if the individual concerned authorises the disclosure of the information to that overseas person. "Authorisation" under the Privacy Act tends to require informed consent. If the protection under the new legislation is to have any real force, the informed and specific nature of the consent will need to be strictly enforced. Otherwise, it will be too simple for agencies to circumvent the policy intent of the legislation (for example by claiming that authorisation arises under broad or legalistic terms and conditions).

iv *Other one-off exceptions*

108 Section 114B(3) of the Privacy Act (permitting the Commissioner to issue transfer prohibition notices) sets out two exceptions:

- (a) A notice cannot be issued if other New Zealand legislation authorises the transfer.
- (b) A notice cannot be issued if the transfer of the information or the information itself is required by any convention or other instrument imposing international obligations on New Zealand.

25 Office of the Privacy Commissioner, "Fact Sheet on Part 11A of the Privacy Act 1993: Transfer of Personal Information Outside New Zealand" (Guidance Resources).

109 These exceptions are straightforward and require little in the way of guidance. It would be useful to have some practical examples of where they occur, but these will emerge over time.

v *Contracts*

110 Contractual provisions governing handling of personal information are not strictly compulsory, but are common. In particular as overseas jurisdictions increasingly require certain standards for data protection (such as having mandatory breach notification requirements), it is becoming more common to see relevant clauses in contracts. Normalising such provisions will have a positive effect on privacy protection in other areas – that is, it is likely they will become more standard even where not strictly required by law.

111 Any contract should ensure that the existing protections in the Privacy Act are recognised and enforceable. However, even if the contract is silent on the point, the New Zealand agency will remain responsible for information that is still within its control.

112 New Zealand agencies must ensure that individuals can still exercise their rights of access and correction of their information, regardless of where in the world the agency chooses to hold the information. If the transfer is to result in the New Zealand agency losing control of the information altogether, that agency is not necessarily required to ensure that the individual's rights are protected. However, the transfer itself (the disclosure of the information) must be justified under the Privacy Act.

113 New Zealand law does contain rules about privity of contract under which only parties to a contract will have rights or obligations under that contract. There is a limited exception to the normal rule that only the parties can enforce contracts. Under subpart 1 of the Contract and Commercial Law Act 2017, third parties can enforce a promise made in a contract for their benefit, even though they are not a party to that contract, unless it appears that the promise was not intended to be

enforceable by the third party. It only applies to promises, contracts or deeds made under New Zealand law, not foreign law.²⁶

114 Standard Contractual Clauses (“SCCs”) have not yet been published by the Privacy Commissioner or other government authority, though this may well prove useful.

vi *CBPRs*

115 New Zealand has not joined or lodged a Notice of Intent to participate in the APEC CBPR system.

vii *Certification, trustmarks and privacy seals*

116 New Zealand has uniform privacy laws. It does not rely on certification, trustmarks or privacy seals.

117 Certification mechanisms, privacy seals and trustmarks delivered in a third country could be relevant considerations for the Privacy Commissioner in deciding whether to issue a transfer prohibition notice. The proposals for the new law have focused on jurisdiction-level comparability with New Zealand law, but it is possible that certification and trustmarks might also be recognised as a valid means for a data exporter to demonstrate compliance with local cross-border data controls. More likely, rather than creating a formal legal status, such mechanisms can provide a degree of assurance when entering into contracts.

118 It is unclear whether the law would accommodate a mechanism of mutual recognition of trustmarks or privacy seals delivered in another jurisdiction.

26 Contract and Commercial Law Act 2017 s 12.

viii *Other data transfer instruments*

119 New Zealand does not have a Binding Corporate Rules system. However, as mentioned earlier, the cloud computing industry has developed a code of practice.²⁷ New Zealand is also an active participant in some of the potentially relevant ISO certification work and some New Zealand companies have achieved certification (eg, with ISO 27018 on cloud computing).

G ENFORCEMENT OF CROSS-BORDER DATA TRANSFER RULES AND INTERNATIONAL CO-OPERATION BETWEEN THE PRIVACY COMMISSIONER AND FOREIGN PRIVACY ENFORCEMENT AUTHORITIES

i *Enforcement of cross-border transfer restrictions*

120 Failure to observe the terms of a transfer prohibition notice is an offence under section 114F of the Privacy Act (that is, it is a criminal act). The offender would be liable on conviction to a fine not exceeding NZ\$10,000. There is no distinction between an individual offender and a corporate offender.

121 If an agency wishes to appeal against a transfer prohibition notice, it can appeal to the specialist tribunal that hears cases under the Privacy Act, the Human Rights Review Tribunal (section 114G). The appeal must be lodged within 15 working days of service of the notice on the agency. Further avenues of appeal would be available to the High Court and beyond.

122 The Privacy Commissioner has not yet issued any transfer prohibition notices, so enforcement of these provisions has not been an issue.

123 The Privacy Commissioner could prosecute an agency for failing to observe the terms of a transfer prohibition notice. This would be a criminal case, brought in the District Court. However, a successful

27 The New Zealand CloudCode “Cloud Computing Code of Practice.

prosecution would not necessarily result in a court order that the agency must then comply with the terms of the notice: it may simply result in a fine for failure to comply. In his briefing to the incoming Minister of Justice in October 2017, Privacy Commissioner John Edwards recommended that the Privacy Commissioner should be empowered to apply to the High Court for a civil penalty to be imposed in cases of serious breaches (up to \$100,000 in the case of an individual and up to \$1 million in the case of a body corporate).²⁸

124 It is also unlikely that the Commissioner could take a case to the Human Rights Review Tribunal to obtain a judicial order requiring the agency to comply. The tribunal only has the jurisdiction that is expressly provided by statute, and neither the Privacy Act nor the tribunal's parent act, the Human Rights Act, provide that jurisdiction. The Commissioner cannot currently be a party to any proceedings in the tribunal. In the same briefing as referred to above, the Commissioner has indicated that he would welcome the opportunity to work with the tribunal and Ministry to develop proposals to address how best to bring cases to the tribunal's attention.

125 It also does not appear that an affected individual, or group of individuals, could take a case to the Human Rights Review Tribunal purely on the basis that the agency had failed to comply with a transfer prohibition notice. Such a failure does not form part of the definition of an "interference with privacy" under section 66 of the Act, which is the trigger for actions in the tribunal, and for any remedies that the tribunal can award.

126 It may be possible for the Commissioner to obtain an injunction in the courts to ensure that information is not transferred in breach of the transfer prohibition notice, but such an action would be novel.

127 No enforcement action has yet been taken by the Privacy Commissioner against any agency based on the conditions under which local information have been transferred to another jurisdiction.

28 Office of the Privacy Commissioner, "Briefing for the Incoming Minister of Justice: Hon Andrew Little" (October 2017).

ii *International co-operation and enforcement by the Privacy Commission with foreign privacy enforcement authorities*

128 The Privacy Commissioner does not have an obligation to ensure regional or international consistency in its decision-making process, when adopting regulatory guidance in the area of international transfers of personal information. However, regional or international consistency is a potentially relevant consideration, as it can affect business to a significant extent. New Zealand is well aware of this dynamic. For instance, it is a member of the Asia Pacific Privacy Authorities (APPA), which is one of several useful regional networks that can help to exchange ideas about effective forms of action, share available guidance and work towards greater consistency to the extent that the local legislation allows for that compatibility.

129 There are no specific provisions in the Privacy Act that require or enable the Privacy Commissioner to develop operational co-operation with the authorities in other jurisdictions. However, the legislation does not contain any insurmountable barriers either. There is a general obligation to maintain confidentiality in section 116, but section 116(2) allows the Commissioner to disclose matters that he thinks ought to be disclosed to give effect to the Act. This could permit the Commissioner to conduct joint investigations with overseas authorities on matters that might breach the New Zealand legislation.

130 The Office of the Privacy Commissioner participates in a number of enforcement co-operation networks or arrangements:

- (a) Global Privacy Enforcement Network (“GPEN”), in which it has been involved every year that the GPEN Sweep has taken place;
- (b) GPEN Alert (an information-sharing system hosted by the US Federal Trade Commission (“FTC”) that aims at co-ordinating international efforts in protecting consumer privacy by sharing information relating to an investigation based on the FTC’s Consumer Sentinel Network);
- (c) APEC Cross-border Privacy Enforcement Arrangement (“CPEA”); and
- (d) Unsolicited Communications Enforcement Network (“UCENet”).

131 The Privacy Commissioner does not participate in the International Conference of Data Protection and Privacy Commissioners (ICDPPC) Enforcement Cooperation Arrangement, neither does it perform an enforcement role under the APEC CBPRs, as New Zealand is not a party to the system.

132 Section 72C of the Act allows the Commissioner to transfer the whole or part of a complaint to an overseas privacy enforcement authority (“PEA”) if the Commissioner believes that the complaint fits more within that overseas authority’s jurisdiction. If the complaint falls within both jurisdictions, the implication is that the authorities could conduct joint investigations or consult with one another as required. The new Privacy Act may further enhance the ability to co-operate with overseas authorities, as the Privacy Commissioner suggested it in the Paper for discussion with the Law Commission on the reform of the Privacy Act – “Enforcement, Compliance, Complaints: A Proposal to Reform the Privacy Act” (2009). It would be beneficial for the law to contain such provisions to enhance the ability of the Privacy Commissioner to work with international colleagues to address privacy problems across borders.

133 The Privacy Commissioner’s office is a member of CPEA and GPEN, and is therefore in principle able and willing to co-operate in the enforcement of privacy laws. In the past, the office has also had a memorandum of understanding with the Australian Privacy Commissioner, which covered information sharing and cross-border co-operation in investigation and enforcement.²⁹

134 The Privacy Commissioner is the sole data protection authority in New Zealand, and has not so far undertaken a joint investigation on privacy issues with other authorities. However, there is no barrier to him doing so. Some authorities, for instance, have complementary functions such as the Department of Internal Affairs’ role in dealing with spam; or

29 Memorandum of Understanding between the Office of the Australian Privacy Commissioner and the Office of the New Zealand Privacy Commissioner (4 September 2006).

NetSafe's role to receive complaints under the Harmful Digital Communications Act.³⁰

135 The Privacy Commissioner has never (at least publicly) undertaken a joint investigation with an authority from another country, though the Commissioner has occasionally co-signed letters with other authorities in response to a particular incident, for instance, the situation involving Google Buzz in 2010³¹ and Google Glass in 2013.³²

136 The Privacy Commissioner has not provided formal assistance to an investigation being undertaken by a PEA from another country. However, he has co-operated with other jurisdictions when required. For example, he received multiple enquiries from European jurisdictions (some forwarded by regulators) into the activities of a New Zealand company, Profile Engine, which republished profiles that had originally been published on Facebook. The Commissioner investigated and came to the opinion that Profile Engine had not breached New Zealand law.

137 The Privacy Commissioner has not taken a formal enforcement action jointly with one of its foreign counterparts and issued common findings against a foreign controller based in multiple jurisdictions. However, the Privacy Commissioner has occasionally liaised with one or more foreign counterparts at a general level while investigating a matter. One example was the Google Street View inquiry, into the unlawful collection of wi-fi data and payload information.³³

30 Daimhin Warner, "Keeping a Low Profile" (Office of the Privacy Commissioner, 12 June 2014).

31 Office of the Privacy Commissioner, "Media Release: Privacy Guardians Warn Multinationals to Respect Laws" (Media Releases and Statements, 20 April 2010).

32 Office of the Privacy Commissioner, "Data Protection Authorities Urge Google to Address Google Glass Concerns and Google's Response" (Media Releases and Statements, 19 June 2013).

33 Office of the Privacy Commissioner, "Google's Collection of WiFi Information During Street View Filming" (Commissioner Inquiries, 14 December 2010).

Jurisdictional Report

REPUBLIC OF THE PHILIPPINES

Reporter: **JJ Disini***

Managing Partner, Disini & Disini Law Office

A INTRODUCTION

1 Republic Act No 10173, otherwise known as the Data Privacy Act of 2012 (“DPA”), was enacted to boost the country’s competitiveness in the international information economy by providing a legal framework by which personal information shall be handled and transferred.¹ As the baseline data privacy law in the Philippines, the DPA generally governs the processing of personal information of the covered data subjects in the country.

2 The three Bills introduced in the House of Representatives and in the Senate emphasised the need to enhance the attractiveness of the Philippines as a business process outsourcing hub. In Representative Susan A Yap’s Explanatory Note to House Bill No 890, she expressed the importance of passing a data privacy law in the Philippines, as countries which have adopted data privacy laws would only outsource information to those who have adopted similar laws. In Representative Roman T Romulo’s Explanatory Note to House Bill No 1554, one of the purposes for introducing the Bill was to amplify the competitiveness of the Philippines in the international economy as a hub for business process outsourcing. Similarly, in Senator Antonio F Trillanes IV’s Explanatory Note to Senate Bill No 355, he highlighted the need to provide a legal framework in relation to the handling and treatment of personal information in the Philippines, as doing so would surely make

* The reporter thanks the National Privacy Commission of the Philippines for their invaluable comments and feedback in the preparation of this report. All errors are this reporter’s own.

1 Explanatory Note to House of Representatives House Bill No 890; Explanatory Note to House of Representatives Bill No 1554; Explanatory Note to S No 355.

the Philippines an attractive option in terms of business process outsourcing.

3 The DPA is not the sole legislation which affords some measure of legal protection to personal data. Republic Act No 10175, otherwise known as the Cybercrime Prevention Act (“CPA”), serves to complement the DPA in terms of protecting data within the Philippine legal framework. The law introduced new cybercrime investigation techniques that allowed law enforcement authorities to go beyond the territorial borders of the country under certain circumstances. Moreover, the Philippine National Police (“PNP”) and the National Bureau of Investigation (“NBI”) were given greater authority to engage in warrantless real-time collection of anonymised traffic data, as well as the explicit imprimatur to secure warrants for the interception of all types of electronic communication. Additionally, the courts were vested with an expanded jurisdiction over the commission of cybercrimes. Thus, as long as the (a) perpetrator is a Filipino; (b) the effects of the cybercrime were felt in the country; (c) if any of the elements of the cybercrime were committed in the country; or (d) if the cybercrime was committed using equipment located in the Philippines, such may be prosecuted in the Philippine courts.

4 Undoubtedly, economic considerations are the primary drivers of cross-border data transfers in the Philippines. Notably, it was the business process outsourcing services industry that served as the primary proponent of the DPA as well as the CPA.

5 It should also be noted that the Philippines has extensive trading ties with the US, as well as members of the European Union (“EU”). As the Philippines is situated between the privacy regimes of both the US and the EU, the Philippines is faced with the prospect of crafting a legal framework that would comfortably accommodate the aforementioned privacy regimes. It comes as no surprise, therefore, that compliance with the cross-border data controls for inbound data from countries following the General Data Protection Regulation (“GDPR”) has a significant impact on Philippine organisations. This impact primarily stems from the fact that these organisations must process the inbound data in accordance with the requirements of the GDPR, which is arguably more stringent compared to the privacy regime of the US.

B GENERAL LEGAL FRAMEWORK OF INTERNATIONAL DATA TRANSFERS

i *International data transfers in national legislation*

a Data Privacy Act of 2012

6 The DPA was enacted to serve as the legal framework on data protection in the Philippines.

7 With respect to enforcing this legal framework, it is the National Privacy Commission (“NPC”) that primarily handles this, including the application of the rules on international data transfers.² The NPC is helmed by the Hon Raymund E Liboro as Commissioner.

8 In August 2016, the NPC issued the Implementing Rules and Regulations of the Data Privacy Act (“DPA IRR”). It has also been regularly issuing circulars providing guidelines on certain requirements of the law.

9 The only applicable provision to cross-border data transfers in the DPA is section 21 thereof:

SEC. 21. *Principle of Accountability.* – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

- (a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party.
- (b) The personal information controller shall designate an individual or individuals who are accountable for the organization’s compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.

10 The Philippines’ approach to liability regarding cross-border transfers is fairly simple: it is the personal information controller who is

2 Implementing Rules and Regulations of Republic Act No 10173 ss 8(d)(3) and 8(d)(4).

responsible for ensuring the protection of personal information under its control or custody – even when such personal information has been transferred to a third party outside of the country for processing. Personal information controllers are required to use contractual or other means to ensure that the third-party entity to whom the personal information is to be transferred for processing provides a comparable level of protection as that of the Philippines.³

11 While the DPA and the DPA IRR do not specifically state the roles of the NPC with respect to international data transfers, they do give the NPC a wide latitude in regulating such transfers.⁴

- (n) Ensure proper and effective coordination with data privacy regulators in other countries and private accountability agents, participate in international and regional initiatives for data privacy protection;
- (o) Negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws;
- (p) Assist Philippine companies doing business abroad to respond to foreign privacy or data protection laws and regulations; and
- (q) Generally perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection.

12 As of this writing, the NPC has yet to issue any advisory or circular that specifically pertains to the implementation of the relevant provision on international transfers.

b Sector-based data transfer restrictions

13 While there are specific laws and regulations that restrict the disclosure of certain pieces of information (see below), the only sector-based data transfer restrictions that exist in the Philippines would be those that pertain to the financial sector.

14 Firstly, Republic Act No 1405, otherwise known as the “Law on Secrecy of Deposits”, prohibits the disclosure of any information

3 Implementing Rules and Regulations of Republic Act No 10173 s 50.

4 Republic Act No 10173 s 7.

regarding a deposit of whatever nature, “except upon written permission of the depositor, or in cases of impeachment, or upon order of a competent court in cases of bribery or dereliction of duty of public officials, or in cases where the money deposited or invested is the subject matter of the litigation”.⁵

15 Secondly, Republic Act No 6426, otherwise known as the “Foreign Currency Deposit Act”, provides that all foreign currency deposits authorised under the aforementioned law are of an absolutely confidential nature.

16 Thirdly, rule 9.3.d of the Revised Rules and Regulations implementing Republic Act No 9160 (“the Anti Money-Laundering Act of 2001”) prohibits covered institutions and their officers from disclosing the fact that a covered or suspicious transaction report was made, the contents thereof, or any other information in relation thereto.

17 Fourthly, Republic Act No 9510, otherwise known as the “Credit Information System Act”, provides for the duty to maintain the confidentiality of credit information.

18 Lastly, subsection X501.7 of the Manual of Regulations for Banks (2017) prohibits the disclosure of foreign currency deposits of clients with any banking institution except upon the written permission of the depositor.

19 The Monetary Board, through the Bangko Sentral ng Pilipinas (“BSP”), is the chief regulator of banking and financial institutions in the Philippines. However, it is not the entity that handles the enforcement of the abovementioned laws. In cases of breach, it is the prosecutors attached under the Department of Justice’s (“DOJ”) National Prosecution Service (“NPS”) that directly handle the prosecution of these cases.

5 Republic Act No 1405 s 2.

c International data transfers by government agencies

20 In the public sector, NPC Circular No 16-02 on “Data Sharing Agreements Involving Government Agencies” includes a similar provision on cross-border transfer of personal data, which is specifically applicable to government agencies:

SECTION 10. *Accountability for Cross-border Transfer of Personal Data.* Each party to a data sharing agreement shall be responsible for any personal data under its control or custody, including those it has outsourced or subcontracted to a personal information processor. This extends to personal data it shares with or transfers to a third party located outside the Philippines, subject to cross-border arrangement and cooperation.

ii Statutory protection of privacy

21 In addition to the DPA, there is a whole gamut of laws that not only regulate data processing but also impose confidentiality restrictions relative to such data. Below is a survey of the relevant legislation on the matter. These statutory impositions should also be taken into account whenever personal information or data are processed in the Philippines.

22 Parenthetically, penal laws are only punishable when committed in the Philippines, unless provided otherwise by the Revised Penal Code or by specific legislation.

a Photo and video voyeurism

23 Republic Act No 9995, otherwise known as the “Anti-Photo and Video Voyeurism Act of 2009”, penalises the act of taking a photo or a video of a person performing sexual acts or any similar activity, or to capture an image of a person’s private area, without the consent of the persons involved and under circumstances in which the person or persons has or have a reasonable expectation of privacy.⁶

6 Republic Act No 9995 s 4(a).

24 The law further penalises the copying, reproduction,⁷ selling, distribution,⁸ publishing or broadcasting⁹ of the images or videos in question (collectively, the “subsequent acts”). The prohibition against these subsequent acts applies regardless of the grant of consent to record a video or take a photo.¹⁰ Additionally, any record, photo or video, or copy thereof, obtained or secured by any person in violation of Republic Act No 9995 shall not be admissible in evidence.¹¹

b Wiretapping

25 Republic Act No 4200, otherwise known as the “Anti-Wiretapping Law”, penalises wiretapping and other violations of the privacy of communications of persons.¹²

c AIDS prevention

26 Republic Act No 8504, also known as the “Philippine AIDS Prevention and Control Act of 1998”, provides for the mechanisms by which individuals who undergo HIV testing may preserve their anonymity and privacy. The law provides that the “[t]he State shall provide a mechanism for anonymous HIV testing and shall guarantee anonymity and confidentiality in the conduct of such tests”.¹³

27 The Implementing Rules and Regulations of Republic Act No 8504 defines “[a]nonymous [t]esting” as an HIV test procedure whereby the identity of the individual being tested is protected. The first mode of anonymous testing – the unlinked anonymous method – tests blood drawn for other purposes for HIV antibodies without the subject’s knowledge and with all identifying data removed. The second mode of anonymous testing – the voluntary anonymous method – tests blood

7 Republic Act No 9995 s 4(b).

8 Republic Act No 9995 s 4(c).

9 Republic Act No 9995 s 4(d).

10 Republic Act No 9995 s 4.

11 Republic Act No 9995 s 7.

12 Republic Act No 4200 s 1.

13 Republic Act No 8504 s 18.

drawn from volunteers who have no identifying information, except a code number which is matched with a similar code of a given test result.

28 In addition to the foregoing, there are also provisions that require maintaining the confidentiality of the records and proceedings involving certain offended parties, as well as children in conflict with the law.

d Minors

29 Republic Act No 9344, otherwise known as the “Juvenile Justice and Welfare Act of 2006”, provides that all records and proceedings involving a child in conflict with the law, from initial contact until final disposition of the case, shall be considered privileged and confidential.¹⁴ The general public shall be excluded during the proceedings, and the records thereof shall not be disclosed directly or indirectly to anyone by any of the parties or the participants in the proceedings for any purpose whatsoever, except to determine if the child in conflict with the law may have his or her sentence suspended or if he or she may be granted probation under the Probation Law, or to enforce the civil liability imposed in the criminal action.¹⁵ Records of a child in conflict with the law shall not be used in any subsequent proceedings for cases involving the same offender as an adult, except when such use shall be beneficial for the offender and upon his or her written consent.¹⁶

30 Additionally, should the child in conflict with the law be subjected to physical and mental examination, the examination results shall be kept confidential unless ordered otherwise by the court.¹⁷

e Women and children

31 Republic Act No 7610, otherwise known as the “Special Protection of Children Against Child Abuse, Exploitation and Discrimination Act”, provides that “at the instance of the offended party, his name may be

14 Republic Act No 9344 s 43.

15 Republic Act No 9344 s 43.

16 Republic Act No 9344 s 43.

17 Republic Act No 9344 s 21(j).

withheld from the public until the court acquires jurisdiction over the case”.¹⁸ This law also makes it unlawful for any editor, publisher, reporter or columnist in case of printed materials, announcer or producer in the case of television and radio broadcasting, producer and director in the case of the movie industry, to cause undue and sensationalised publicity of any case of violation of this Act which results in the moral degradation and suffering of the offended party.¹⁹

32 Republic Act No 9262, otherwise known as the “Anti-violence Against Women and their Children Act of 2004”, provides for the duty to maintain the confidentiality of the records pertaining to the offended parties.²⁰ Similarly, the Supreme Court Rule on Violence Against Women and their Children²¹ provides for that same level of protection for women and children.

33 As a corollary, the Supreme Court, through the case of *People of the Philippines v Melchor Cabalquinto*,²² the real names of rape victims shall not be disclosed in court decisions. The personal circumstances of the victims or any other information tending to establish or compromise their identities shall likewise be withheld.

f Financial information

34 The Philippines also has legislation in place providing for the confidentiality of financial information. Republic Act No 1405, otherwise known as the “Bank Secrecy Law”, provides for the duty to maintain the confidentiality of information relating to deposits, as well as the exceptions thereto.

35 Another recognised exception to the Bank Secrecy Law is section 8 of Republic Act No 3019, otherwise known as the “Anti-Graft and Corrupt Practices Act”. Essentially, should a public official be found to

18 Republic Act No 7610 s 29.

19 Republic Act No 7610 s 29.

20 Republic Act No 9262 s 44.

21 AM No 04-10-11-SC.

22 GR No 167693, 19 September 2006.

have unexplained wealth during his incumbency, such finding may be a ground for dismissal or removal.

36 Republic Act No 9160 as amended by Republic Act No 10365, otherwise known as the “Anti-Money Laundering Act”, as amended, provides that the Anti-Money Laundering Council may inquire into a bank account upon order of any competent court in cases of violation of the Anti-Money Laundering Act, it having been established that there is probable cause that the deposits or investments are related to unlawful activities as defined in section 3(i) of the Act, or a money laundering offence under section 4 thereof.²³

37 Unlike the Bank Secrecy Law, Republic Act No 6425, otherwise known as the “Foreign Currency Deposit Act”, as amended, grants absolute confidentiality to foreign currency deposit accounts. Moreover, Presidential Decree No 1246 provides that foreign currency deposit accounts may only be looked into with the written permission of the depositor.²⁴ It should be noted that this grant of confidentiality is absolute. Not surprisingly, the law also exempts foreign currency deposits from writs of attachment or garnishment, or other processes of the court. Notwithstanding the seeming premium granted to foreign currency deposits in terms of confidentiality, the exceptions provided under the Anti-Money Laundering Act shall also apply to cases involving foreign currency deposits.

38 Given the array of laws providing for the confidentiality of financial information, it stands to reason that the law would also require maintaining the confidentiality of tax records as well. Section 270 of the National Internal Revenue Code (“Tax Code”) states that information about a taxpayer’s tax return shall be afforded the highest degree of confidentiality. Any personnel of the Bureau of Internal Revenue (“BIR”) divulging any information in the tax return can be charged criminally and administratively by a fine of not more than PHP2,000, or an imprisonment of not less than six months nor more than five years or both.

23 Republic Act No 9160 s 11.

24 Presidential Decree No 1246 s 2.

39 Further, section 6(F)(3) of the Tax Code mandates banks and financial institutions to ensure confidentiality in the handling of tax information in their possession.

iii *Constitutional protections*

40 The Philippine Constitution expressly recognises the concept of privacy. The latest iteration of the same – the 1987 Constitution – provides:²⁵

Section 3. (1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law.

(2) Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding.

41 This provision is brought forward from similar provisions in the 1935 and 1973 Constitutions, under Article III section 1(5) and Article IV section 4(1) respectively, and has remained relatively unchanged.

42 However, this provision does not speak squarely to data protection or privacy. It merely mentions privacy as to “communication”, not as to personal data or information at large. Moreover, because of section 3(2) thereof, it is applied in conjunction with the right against unreasonable searches and seizure, which is the “preceding section” mentioned therein.

43 Notwithstanding the want of express basis in the Constitution on this point, there have been decisions made by the Philippine Supreme Court which interpret data privacy as a constitutional right.

44 In the landmark decision of *Jesus P Morfe v Amelito R Mutuc*²⁶ (“*Morfe*”), a law requiring public officials to file an annual statement of assets, liabilities, income and expenses was challenged “for being violative of due process ... as an unlawful invasion of the constitutional right to privacy, implicit in the ban against unreasonable search and seizure construed together with the prohibition against self-incrimination”.

25 The 1987 Constitution of the Philippines Art III.

26 GR No 20387, 31 January 1968.

Preliminarily, the court observed that the right to privacy may be found in the Constitution: expressly, under the inviolability of the privacy of communication, and implicitly, in the search and seizure clause and the liberty of abode. But as to the aspect of privacy allegedly infringed by the assailed law, the court found no local precedent and looked to the US case of *Griswold v Connecticut*²⁷ (“*Griswold*”). The court, citing and adopting *Griswold*, held that “[t]he right to privacy as such is accorded recognition independently of its identification with liberty; in itself, it is fully deserving of constitutional protection”.

45 Despite adopting *Griswold*, the court nonetheless sustained the assailed law, ruling that a rational relationship exists between the required disclosure of information and the objective of the statute, which is to repress graft and corrupt practices.

46 Under the *Griswold* interpretation, the right to privacy is penumbral – not mentioned expressly in the US Constitution, but may be inferred from the other constitutional guarantees. The same situation avails in the Philippines, as the *Morfe* decision clearly declares, although it is less nebulous at least as to privacy of communication which the Philippine Constitution expressly guarantees.

47 It will be noted that the Philippines was once a colony of the US in the early 20th century, and that its government and constitution is modelled after the latter’s. Thus, American jurisprudence retains some persuasive weight in this jurisdiction (*Alzua v Johnson*;²⁸ *In re Max Shoop*),²⁹ more so in relation to the constitutional guarantees against unreasonable search and seizure (*People v Marti*³⁰ (“*Marti*”)).

48 In *Blas F Ople v Ruben D Torres*,³¹ the Philippine President issued an administrative order adopting a National Computerized Identification Reference System enabling a decentralised reference system between government agencies. The court struck down the order as violative of the

27 381 US 479 at 484 (1965).

28 GR No L-7317, 31 January 1912.

29 19 OG 766, 29 November 1920.

30 GR No 81561, 18 January 1991.

31 GR No 127685, 23 July 1998.

constitutional right to privacy, for fear of the potential for misuse of such extensive records. The court also found that the administrative order was not narrowly drawn.

49 In *Jose Jesus M Disini, Jr v Secretary of Justice*³² (“*Disini*”), petitioners assailed the CPA for violating the constitutional right to privacy. The court remarked that the right to privacy was institutionalised in the 1987 Constitution as a facet of the right against unreasonable searches and seizures.

50 As to the right to data privacy (independent of the DPA), the court, in *Disini*, adopted the discussion made in the US case of *Whalen v Roe*³³ (“*Whalen*”), on the various aspects of privacy. Citing *Whalen*, the court explained that there are two categories of privacy: decisional privacy and informational privacy. Further, informational privacy itself has two aspects: the right not to have private information disclosed, and the right to live freely without surveillance and intrusion. Of these two aspects of information privacy, the former, the right not to have private information disclosed, speaks more closely to the right to data privacy.

51 It will be noted that these cases concern only state actions. Jurisprudence holds that constitutional rights may only be asserted against the State, and not against private persons (*Marti*). Privacy, as a constitutional right, then is delimited to public infringements.

52 However, there have been cases between private persons that have been fought on the grounds of privacy. It will be noted that these are premised on other sources of the right to privacy outside the Constitution.

53 In *Spouses Bill and Victoria Hing v Alexander Choachuy*,³⁴ the plaintiffs filed an action against the defendants based on Article 26(1) of the Civil Code, which provides for the granting of relief where one prides into the privacy of another’s residence, among other things.

32 GR No 203335, 11 February 2014.

33 429 US 589 (1977).

34 GR No 179736, 26 June 2013.

54 The plaintiffs and the defendants were neighbours with adjacent properties. The defendants set up two video surveillance cameras directed at the plaintiff's property and took pictures of the plaintiffs' ongoing construction. The court held that the plaintiffs had a reasonable expectation of privacy in their property, and "that the installation of video surveillance cameras directly facing petitioners' property or covering a significant portion thereof, without their consent, is a *clear violation of their right to privacy*" (emphasis added).

55 In *Rhonda Ave S Vivares v St Theresa's College*³⁵ ("*Vivares*"), photographs of two graduating high school students, uploaded by them on Facebook, were used by their school's administration as basis for denying them participation in their graduation rites. The said photos depicted the two engaged in smoking, drinking, wearing scanty clothing and other "immoral acts". These pictures were made known to the school by fellow students who were "friends" with the two on Facebook. The plaintiffs filed a petition for the issuance of a Writ of Habeas Data.

56 The *Writ of Habeas Data* is a remedy developed by the Supreme Court to protect the right to *informational privacy*. If warranted, "the court [through the writ] shall enjoin the act complained of, or order the deletion, destruction, or rectification of the erroneous data or information and grant other relevant reliefs as may be just and equitable".³⁶

57 *Vivares* recognised the individual's right to informational privacy, as one of the three strands of privacy, and the right's precarious position considering modern technology. The issuance of the writ in this case was premised on whether a reasonable expectation of privacy was violated. In construing whether such expectations exist, the court considered that the subject photographs were obtained by the school through Facebook, which the court described as an online social network ("OSN"). The court appreciated that although OSNs are generally used to share information and connect with other members of the same platform, where privacy settings exist, as in the case of Facebook as found by the

35 GR No 202666, 29 September 2014.

36 AM No 08-1-16-SC s 16.

court, a reasonable expectation of privacy may exist. The expectation must be coupled with some overt act by the individual to manifest his intention to bring the subject information into the protected zone of privacy.

58 Ruling on the matter at hand, the court found that the students, in their use of Facebook privacy settings, did not have a reasonable expectation of privacy over the subject photographs. It found that the students did not limit the disclosure of the said photographs, which were viewable to their Facebook friends or even the public at large. It also held that sharing under the “Friends Only” setting does not confer a reasonable expectation of privacy, considering the social dynamics of the Facebook platform. Finding no violation of privacy, the court denied the petition.

iv *International engagement*

a ICCPR and optional protocol

59 It is worth emphasising that the Philippines has signed and ratified the International Covenant on Civil and Political Rights (“ICCPR”). Moreover, the Philippines has also signed and ratified the First Option Protocol to the ICCPR (“CCPR-OP1”).

b Free trade agreements

60 With regard to free trade agreements (“FTAs”), the Philippines is currently a signatory to the following FTAs: Association of Southeast Asian Nations (“ASEAN”) Free Trade Area; ASEAN Trade in Goods Agreement (“ATIGA”); European Free Trade Association (“EFTA”); and Japan-Philippines Economic Partnership Agreement (“JPEPA”).

61 The EFTA to which the Philippines is a signatory appears to have provisions covering the transfer of personal data among the signatories. The relevant provision under Annex XIII is quoted hereunder:

Article 7

Transfers of Information and Processing of Information

(1.) No Party shall, subject to its domestic laws, rules and regulations, take measures that prevent transfers of information into or out of the

Party's territory or the processing of financial information, including transfers of data by electronic means, or that, subject to importation rules consistent with international agreements, prevent transfers of equipment, where such transfers of information, processing of financial information or transfers of equipment are necessary for the conduct of the ordinary business of a financial service supplier of another Party.

(2.) Nothing in this Article restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of Chapter 6 of the Agreement.

62 Notably, the provisions of the EFTA do not seem to override the restrictions on cross-border data transfers enshrined in the national laws of the parties to the EFTA.

c Regional data protection frameworks

I APEC, CPEA AND CBPR

63 The Philippines is an Asia-Pacific Economic Cooperation ("APEC") Member economy. As such, it has joined the APEC Cross Border Privacy Enforcement Arrangement ("CPEA"), which is the government backstop enforcement network developed for the Cross-Border Privacy Rules ("CBPR"). Administrators of the CPEA confirmed the NPC's status as a privacy enforcement authority ("PEA") for the Philippines on 7 December 2017.³⁷

II ASEAN

64 It should be noted that the Philippines is a member of the ASEAN Economic Community ("AEC").³⁸ Being a member of the AEC, it has

37 National Privacy Commission, "PH Strengthens Extraterritorial Reach through the APEC Cross Border Privacy Enforcement Arrangement" <<https://privacy.gov.ph/ph-strengthens-extraterritorial-reach-apec-cross-border-privacy-enforcement-arrangement/>> (accessed 1 February 2018).

38 ASEAN Business Advisory Council Philippines, "The ASEAN Economic Community" <<http://www.aseanbac.ph/index.php/page/view/asean-economic-community>> (accessed 1 February 2018).

taken measures to follow up on the adoption of the ASEAN Framework on Personal Data Protection, such as the enactment of the DPA.³⁹

III IMPACT OF GDPR

65 It is, however, worth mentioning that the extraterritorial effects of the European GDPR may have a significant impact on the data processing activities of businesses in the Philippines. Under the DPA, personal information originally collected from residents of foreign jurisdictions is excluded from the application of the law if collected in accordance with the laws of those foreign jurisdictions.⁴⁰ As such, businesses processing information from jurisdictions that are under the GDPR would have to check if the data are collected in accordance with the GDPR.

C DEFAULT POSITION, SCOPE AND TERRITORIAL EFFECT DATA PRIVACY ACT OF 2012

i *Default position on data transfers*

66 As a general rule, international data transfer is authorised under this jurisdiction. There are also no data export restrictions. In other words, the DPA does not restrict cross-border transfers. However, it does impose the responsibility to ensure the confidentiality, integrity and accessibility of the personal information on the personal information controller.

ii *Extraterritorial scope and effect*

67 The provision on international data transfers, specifically section 21 of the DPA, may be deemed extraterritorial in scope, as the liability for

39 Graham Greenleaf, "ASEAN's 'New' Data Privacy Laws: Malaysia, the Philippines and Singapore" 116 Privacy Laws & Business International Report 22 (April 2012). See also ASEAN Telecommunications and Information Ministers Meeting, "Framework on Personal Data Protection" <<http://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf>> (accessed 1 February 2018).

40 Republic Act No 10173 s 4(g).

personal information transferred outside of the Philippines attaches to the personal information controller.

68 With respect to the above, the DPA requires personal information controllers and processors to procure the valid consent of the data subjects for all types of processing of the latter's personal information. The term "processing" includes the transfer of personal information. The data subject must, therefore, be informed and must thereafter give their consent to the transfer of his or her personal information to offshore locations.

69 The foregoing requirements apply to the processing of all types of personal information and to any natural or juridical person involved in such processing, including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that is located in the Philippines or those who maintain an office, branch or agency in the Philippines. This is subject to the exceptions under section 4(a) to section 4(g) of the DPA.

70 The DPA also has extraterritorial application and shall apply to an act done or practice engaged in outside the Philippines by an entity if:⁴¹

- (a) The act, practice or processing relates to personal information about a Philippine citizen or a resident;
- (b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following:
 - (1) A contract is entered in the Philippines;
 - (2) A juridical entity unincorporated in the Philippines but has central management and control in the country; and
 - (3) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and
- (c) The entity has other links in the Philippines such as, but not limited to:

41 Republic Act No 10173 s 6.

- (1) The entity carries on business in the Philippines; and
- (2) The personal information was collected or held by an entity in the Philippines.

iii *Type of organisations covered by Data Privacy Act of 2012*

71 The rule enshrined therein covers all operators in the private sector. The law does not make any distinctions with respect to specific personal information controllers. In the eyes of the law, all personal information controllers are equally liable should any of them violate the provisions of the DPA.

72 As a corollary, the DPA does not distinguish between controllers and processors or intermediaries, as accountability for the personal information transferred rests solely upon the personal information controller.

73 As regards the business process outsourcing (“BPO”) industry, there exists an exemption under section 4 of the DPA with regard to the personal information of foreign residents lawfully collected abroad. However, it should be clarified that such exemption applies to the personal information and not to the organisation. In other words, while the personal information of foreign residents – lawfully collected abroad – is not covered by the DPA, the organisation processing such information still has to comply with the DPA, especially with respect to data subjects who do not qualify under such exemption, in addition to the security requirements set forth in the aforementioned law.⁴²

iv *Type of data covered by Data Privacy Act of 2012*

a *Definition of Personal Information under the Data Privacy Act of 2012*

74 The DPA will apply if the data being transferred or processed are personal information as defined under the law. Under the DPA and the

42 On the exact scope of the exemption, see paras 78–81 below.

DPA IRR issued by the NPC, “Personal Information” refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

b Processing of certain information exempt from requirement of consent

75 Despite the seemingly grand scope of the DPA, there are still certain items that are beyond its scope. The only kinds of personal information that are exempt from the requirement of procuring the data subject’s valid consent prior to transfer would be those types of processing and information enumerated under section 4 of the DPA:

- (a) Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:
 - (1) The fact that the individual is or was an officer or employee of the government institution;
 - (2) The title, business address and office telephone number of the individual;
 - (3) The classification, salary range and responsibilities of the position held by the individual; and
 - (4) The name of the individual on a document prepared by the individual in the course of employment with the government;
- (b) Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;
- (c) Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit;
- (d) Personal information processed for journalistic, artistic, literary or research purposes;
- (e) Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law

enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in this Act shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);

(f) Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; and

(g) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.

76 Notably, section 4(g) of the DPA places personal information lawfully collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions and which is being processed in the Philippines beyond the ambit of the DPA. However, the personal information of foreign residents which is being processed in the Philippines remains within the mantle of protection provided by the CPA.

77 Interestingly, the DPA does not provide a mechanism through which the public can claim or have their exemption status approved. Given the language of the law, the exemptions will be a matter of defence for the persons claiming the same. They will have to be pleaded and proved in a court of law, pursuant to the provisions of the Rules of Court.

c Processing of personal information from residents of foreign jurisdictions

78 It should be noted that the last paragraph of section 4 of the DPA seems to embody the rule that the DPA does not protect the data privacy rights of foreign nationals. It appears that the BPO sector would be free to process the personal information of foreign nationals without needing to protect their privacy.

79 First, it should be noted that if the personal data are collected from such foreign national in violation of his domestic law, then its transfer to the Philippines will not exempt such data from the DPA's coverage. Second, the CPA expressly provides protection under the crime of "Identity Theft" defined in section 4(b)(3), as follows:

Computer-related Identity Theft. – The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right: *Provided*, That if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

80 In the CPA's Implementing Rules and Regulations, the term "identifying information" is defined as follows:⁴³

Identifying information refers to any name or number that may be used alone or in conjunction with any other information to identify any specific individual, including any of the following:

1. Name, date of birth, driver's license number, passport number or tax identification number;
2. Unique biometric data, such as fingerprint or other unique physical representation;
3. Unique electronic identification number, address or routing code; and
4. Telecommunication identifying information or access device.

81 Clearly, the expansive definition of "identifying information" means that the unauthorised processing of personal information including its intentional collection can be prosecuted under the CPA. It can be argued, in fact, that the CPA provides greater protection than the DPA since the penalty for identity theft is *prision mayor*⁴⁴ or from six to 12 years for every count.

d Anonymised information

82 Considering that the DPA is concerned with protecting the privacy of the data subject, anonymised information is naturally excluded from

43 Rules and Regulations Implementing Republic Act No 10175 s 3(y).

44 Revised Penal Code (Act No 3815) Art 27.

the scope of application of the law. The legal basis for this exception is derived from section 3(g) of the DPA, which defines personal information as any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding such information, or when put together with other information would directly and certainly identify an individual. Anonymised information necessarily falls outside of this definition, while pseudonymised and encrypted data do not. The latter categories of data, when put together with other information, would still directly and certainly identify an individual.

83 Curiously, the NPC does not play a role in the assessment of whether data are anonymised. The fact that data are anonymised may be raised during an audit to claim that such information is not covered by the DPA. As of this writing, the NPC has not published any guidance on whether anonymised and pseudonymised data are truly beyond the scope of the DPA.

84 The NPC has the power to issue an opinion as to whether a certain type of information is sufficiently anonymised or encrypted so as to remove it from the ambit of personal information. However, it should be noted that the courts may choose to invalidate the opinion issued by the NPC if they find that this is contrary to law. According to Advisory Opinion No 2017-27 of the NPC, information is considered anonymous when the same “does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable”.⁴⁵ It should be noted that, in this opinion issued by the NPC, the discussion in Opinion 05/2014 on Anonymization Techniques of the Article 29 Data Protection Working Party of the European Commission with regard to was quoted with approval, to wit:

... to anonymise any data, the data must be stripped of sufficient elements such that the data subject can no longer be identified. More precisely, the data must be processed in such a way that it can no longer be used to identify a natural person by using ‘all the means likely reasonably to be used’ by either the controller or a third party. An important factor is that

45 Regulation (EU) 2016/679 Recital 26.

the processing must be irreversible ... The focus is on the outcome: that data should be such as not to allow the data subject to be identified via ‘all’ ‘likely’ and ‘reasonable’ means. Reference is made to codes of conduct as a tool to set out possible anonymisation mechanisms as well as retention in a form in which identification of the data subject is ‘no longer possible’.⁴⁶

...

An effective anonymisation solution prevents all parties from singling out an individual in a dataset, from linking two records within a dataset (or between two separate datasets) and from inferring any information in such dataset. Generally speaking, therefore, removing directly identifying elements in itself is not enough to ensure that identification of the data subject is no longer possible. It will often be necessary to take additional measures to prevent identification, once again depending on the context and purposes of the processing for which the anonymised data are intended.

...

It must be clear that ‘identification’ not only means the possibility of retrieving a person’s name and/or address, but also includes potential identifiability by singling out, linkability and inference. Furthermore, for data protection law to apply, it does not matter what the intentions are of the data controller or recipient. As long as the data are identifiable, data protection rules apply.⁴⁷

D LEGAL BASIS

85 Under section 3(b) of the DPA, consent refers “[t]o any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her”. According to the same provision, “[c]onsent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so”.

46 See Article 29 Data Protection Working Party, “Opinion 05/2014 on Anonymisation Techniques”, 10 April 2014, s.2.1 for the definition in the EU legal context.

47 See Data Protection Working Party, “Opinion 05/2014 on Anonymisation Techniques”, 10 April 2014, s.2.2.2 on potential identifiability of anonymised data.

86 The consent of the individual is necessary to transfer his or her data. Under the DPA, the processing of information may include its transfer or disclosure.⁴⁸ However, the law also provides instances where consent may not be necessary for such transfer or disclosure. What the law does, in cases of transfers, is to make the transferor accountable for the personal information that it transfers whether domestically or internationally.⁴⁹ Data transfers are not subject to notification or approval of the NPC unless the same include automated data processing.⁵⁰

87 It should be noted that there are other legal bases for international data transfers provided in the law. Under the DPA, the following are also bases for the processing of personal information which may include its transfer:⁵¹

- (a) the processing of personal information is necessary and is related to the fulfilment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
- (b) the processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
- (c) the processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfil functions of public authority which necessarily includes the processing of personal data for the fulfilment of its mandate; or
- (d) the processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data are disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

48 Republic Act No 10173 s 3(j).

49 Republic Act No 10173 s 21.

50 Implementing Rules and Regulations of Republic Act No 10173 s 48.

51 See Republic Act No 10173 s 12.

E DATA LOCALISATION⁵²

88 As regards data localisation, there are no general law requirements on the same in this jurisdiction. However, the DPA does provide some measure of regulation for cross-border transfers, as seen above.

89 Notably, the DPA does not require personal information controllers or processors to keep copies of the transferred data within the Philippines. However, certain regulatory agencies have audit and supervisory powers and may therefore subject an entity to an examination. In these cases, the entities will have to show the regulators copies of the transferred data. For example, the BSP has the power to conduct examinations over banks. Regular or periodic examinations shall be done once a year. Special examinations may be conducted more frequently, when authorised by the Monetary Board by an affirmative vote of five members.

90 Further, it should be noted that the BSP allows banks and non-banks to engage the services of third-party service providers, either domestic or offshore, for back-up and data recovery operations. The banks and non-banks are not required to have the BSP approve their choice of third-party service providers. Nonetheless, “records and information on back-up operation centers and data recovery sites arrangements of banks and non-bank must be made available to BSP examiners during regular examination for purposes of ascertaining that such arrangements are updated and effective”.⁵³

91 The Secretary of the Department of Labor and Employment (“DOLE”) and his duly authorised representatives also have the authority to exercise visitorial powers under Article 128(a) of the Labor Code of the Philippines. The visitorial power grants to the said DOLE officials access to an employer’s records and premises at any time of the day or night whenever work is being undertaken therein, and the right to copy

52 “Data localisation requirements” may be broadly understood here as the prohibition against transfers of personal data without official approval or permit, even if data subjects have consented to the transfer.

53 Bangko Sentral ng Pilipinas Memorandum, 22 January 2004.

from such records, to question any employee and investigate any fact, condition or matter which may be necessary to determine violations or which may aid in the enforcement of the Labor Code and of any labor law, wage order or rules and regulations issued pursuant thereto.

92 The Tax Code also authorises the Commissioner, or his representatives, to examine a taxpayer's records and books. Section 5 of the Tax Code states that:

In ascertaining the correctness of any return, or in making a return when none has been made, or in determining the liability of any person for any internal revenue tax, or in collecting any such liability, or in evaluating tax compliance, the Commissioner is authorized:

(A) To examine any book, paper, record, or other data which may be relevant or material to such inquiry ...

F DATA TRANSFER MECHANISMS

i *Preliminary issues*

93 Being situated between two competing privacy regimes certainly puts the Philippines in a unique position. Considering the great disparity between these two regimes, organisations based in this jurisdiction, especially those who regularly transfer data overseas, are hard-pressed to comply with the requirements of both the EU and US privacy frameworks. Should these organisations fail to do so, they risk losing valuable markets overseas.

94 As the DPA IRR were only released in 2016, organisations are still in the process of fully aligning their internal policies and procedures with the DPA. Such internal policies and procedures would naturally include the mechanisms by which data are transferred. In order not to hamper operations while they are in the process of complying, organisations have opted to continue using the data transfer mechanisms they have been using prior to the enactment of the DPA.

95 In view of the above factual circumstances, it is difficult to determine at this point whether there is a general demand for transfer instruments that would facilitate interoperability between countries and maybe even outside of Asia. However, given that there are multinational

companies within this jurisdiction that operate globally, it stands to reason that they would spearhead the development and adoption of these transfer instruments. Incidentally, it is worth noting that the DPA does promote interoperable data transfers, for, as previously mentioned, data transfer restrictions are conspicuously absent in the DPA.

96 Be that as it may, however, in a bid to simplify the making of a local entity liable for breaches in cross-border data transfers, section 21 of the DPA makes the local personal information controller liable even if the data breach was attributable to the personal information processor located overseas, with such processor being the recipient of the data.⁵⁴

97 Public authorities in the Philippines have yet to officially endorse any means of self-regulation. However, in terms of data protection, information security and process improvement, complying with the standards laid down by the International Organization for Standardization (“ISO”) and the engagement of external auditors for assessing operational gaps are some of the means by which organisations in this jurisdiction undertake self-organisation or self-certification.

ii “Adequacy findings” and white lists

98 The DPA authorises data transfers to jurisdictions that have laws establishing adequate or comparable data protection standards. However, this is not a prerequisite for such transfer. Transfer may also be made to countries which do not provide a comparable level of protection as the DPA, because responsibility for such protection rests on the personal information controller who made the transfer.

99 In conformity with the law, the data exporter is to use contractual or other reasonable means to ensure that proper safeguards are in place, to ensure the confidentiality, integrity and availability of the personal data processed, prevent its use for unauthorised purposes, and generally, comply with the requirements of the DPA, its implementing rules and regulations, and the issuances of the NPC.

54 Republic Act No 10137 s 21.

100 As previously mentioned, the DPA does not list substantive standards to establish that the law of another jurisdiction establishes comparable data protection standards. Under section 7(q), the NPC may generally perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection, under which may fall the authority to publish criteria to determine and recognise whether another jurisdiction has established comparable data protection standards.

101 Notably, the NPC has not implemented a cost benefit analysis of “adequacy” decisions and white or black lists since these are still inexistent.

iii *Consent as exception to existence of privacy safeguards overseas*

102 There appears to be no prohibition against the use of consent as a waiver to the requirement of existing privacy safeguards in the country of destination. In cases of cross-border transfers, the DPA appears to be more concerned as to whether the controller or processor complies with Philippine laws rather than the laws of the country of destination.⁵⁵ This being said, the law does not lay down any specific requirements except that consent, if used as a basis for processing, must be freely given, specific, informed and evidenced by written, electronic or recorded means.⁵⁶ Note that the NPC has not given any guidance to this effect.

iv *Other one-off exceptions*

103 In cases of transfer from the Philippines, the DPA requires the controller to comply with Philippine law but does not mention compliance with the law of the country of destination. Hence, it cannot be determined whether the other exceptions to the requirement of privacy safeguards by the data importer or in the country of destination are accepted under Philippine law.

55 Republic Act No 10173 s 21.

56 Republic Act No 10173 s 3(b).

v *Contracts*

104 The DPA recognises that, in the course of ordinary operations, entities may transfer personal information to other entities (see sections 15, 20(e) and 21). However, it does not provide for any specific modes under which these transfers must operate. The principle of accountability under section 21 merely provides that a controller is responsible for personal information under its control and custody, including that which has been transferred to third parties for processing. Further, section 21(a) requires the controller to use contractual or other reasonable means to provide a comparable level of protection while information is being processed by a third party.

105 The DPA IRR, however, goes into more detail. It makes out two broad types of data transfer arrangements, (a) outsourcing and (b) data sharing, with specific provisions for each.

a *Outsourcing contracts*

106 Section 3(f) of the DPA IRR defines outsourcing as the disclosure or transfer of personal data by a controller to a processor, and under section 44 of the same, processing by a processor pursuant to the instructions of a controller shall be governed by a contract (outsourcing and subcontracting agreement). Section 44(b) provides that the contract must contain stipulations that oblige the processor to:

- (a) process personal data only upon the documented instructions of the controller;
- (b) ensure that an obligation of confidentiality is imposed on persons doing the processing;
- (c) implement appropriate security measures and comply with the DPA;
- (d) not engage another processor without prior instruction from the controller;
- (e) assist the controller in complying with requests from data subjects relative to the exercise of their rights;
- (f) assist the controller in complying with the DPA, considering the nature of the processing and information available to the processor;

- (g) at the instruction of the controller, delete or return all personal data after the completion of the processing services;
- (h) make available to the controller information necessary to demonstrate compliance; and
- (i) inform the controller if, in its opinion, an instruction, violates the DPA.

107 An outsourcing contract is also considered a security measure under section 26(f) of the DPA IRR. Hence, even in cases where scope exemptions under section 5 thereof avail, the controller must conclude an outsourcing agreement since scope exemptions do not extend to security obligations. For example, personal information collected from residents of foreign jurisdictions in accordance with the laws of the said jurisdictions is exempt from the law (section 4(g) of the DPA and section 5(f) of the DPA IRR). However, as discussed, outsourcing activities processing the same must be governed by a contract. This is likely the case in cross-border data transfers.

b Data sharing agreements

108 Section 3(f) of the DPA IRR defines data sharing as disclosure or transfer to a third party of personal data under the custody of a controller or a processor upon the instructions of a controller. Further, the term expressly excludes outsourcing. Necessarily, data sharing is transfer to a controller. Under section 20(b) of the DPA IRR, data sharing in the private sector shall be covered by a data sharing agreement if the data sharing is done for commercial purposes. The DPA IRR merely requires that the agreement establish adequate safeguards for data privacy and security, and uphold the rights of data subjects. The agreement is subject to review by the NPC *motu proprio* or upon complaint of the data subject. There is no clear standard for what constitutes “adequate safeguards”. The rules on data sharing involving government agencies (NPC Circular 16-02) are more precise as to what data sharing agreements must contain. However, the required contents speak of disclosures about the processing activity, rather than prescribing any protective measures.

109 These outsourcing and data sharing agreements are intended to provide data subjects with protection. However, the DPA and the DPA IRR are silent as to how data subjects may enforce any of these

contractual rights. There is no requirement to provide a third-party beneficiary clause.

110 The doctrine of privity is recognised in this jurisdiction, and is provided for by law. However, the enforcement of contractual rights by a third person may lie if the contracting parties clearly provided for such rights in the contract. Article 1311 of the Civil Code provides:

Contracts take effect only between the parties ...

If a contract should contain some stipulation in favor of a third person, he may demand its fulfillment provided he communicated his acceptance to the obligor before its revocation. A mere incidental benefit or interest of a person is not sufficient. The contracting parties must have clearly and deliberately conferred a favor upon a third person.

111 However, even without stipulations *pour autrui*, the DPA itself already provides data subjects with considerable protection and allows them to assert their rights over data transfers involving their information, notwithstanding privity. Data subjects are given a wide array of rights, which include the right to damages and the right to block processing. The principle of accountability also extends the scope of protection granted to the data subject, and holds processors liable for information even if they have transferred the same to third parties.

112 Although the DPA IRR prescribes mandatory contractual stipulations, the regulatory authority has yet to publish any standard language or wording for the same. If several Asian countries jointly adopt standard clauses, that would be very useful to companies such as small and medium-sized enterprises.

113 Although the law itself does not require the conclusion of a data import-export contract, considering the rights and protection it grants to data subjects, such a contract would be the prudent approach. In such a case where, because of the principle of accountability, a controller remains responsible for breaches committed by its outsource, contractual clauses, which may include security obligations and indemnity provisions, would be desirable.

vi *CBPRs*

114 As the Philippines has now joined the APEC CPEA, the next step is, according to Chairman Raymund Liboro, to convene local stakeholders for the purpose of building consensus around formally joining the APEC CBPR.⁵⁷

vii *Certification, trustmarks and privacy seals*

115 Currently, the DPA does not provide for certification to demonstrate compliance similar to that contemplated under Article 42 of the GDPR. However, there is no prohibition from adopting a similar mechanism. The NPC (the regulatory agency) may conceivably issue rules to accommodate such a scheme (*eg*, rules defining certifying bodies).

viii *Other data transfer instruments*

116 The DPA (see section 7(j)) speaks of privacy codes voluntarily adhered to by controllers, which may include private dispute resolution mechanisms for complaints against any participating personal information controller. This concept is relatively unexplored. The law makes little discussion of it, and no implementing rules have been issued addressing the matter precisely yet, compared to the extensive provisions in Chapter IV section 5 and Chapter V on data transfer instruments of the GDPR.

57 National Privacy Commission, “PH Strengthens Extraterritorial Reach through the APEC Cross Border Privacy Enforcement Arrangement” <<https://privacy.gov.ph/ph-strengthens-extraterritorial-reach-apec-cross-border-privacy-enforcement-arrangement/>> (accessed 1 February 2018).

G INTERNATIONAL CO-OPERATION BETWEEN NATIONAL PRIVACY COMMISSION AND FOREIGN PRIVACY ENFORCEMENT AUTHORITIES

i *Co-operation with foreign PEAs in areas other than enforcement*

117 The DPA enables the NPC to develop operational co-operation with the PEAs in other jurisdictions. This leeway is granted to the NPC through section 7(n)⁵⁸ and section 7(o)⁵⁹ of the DPA.

118 As of this writing, the NPC has yet to sign any bilateral or multilateral agreement with the PEAs of other jurisdictions for the purpose of implementing privacy laws. However, it should be noted that the NPC is clothed with sufficient authority to do so, as evidenced by the express provisions⁶⁰ of the DPA.

119 As regards the obligation to ensure regional or international consistency when adopting regulatory guidance in terms of international data transfers and when making decisions that may affect organisations with cross-border operations, neither the DPA nor the DPA IRR provide any specific guidance on these matters. However, the NPC is mandated to “[e]nsur[e] proper and effective coordination with data privacy regulators in other countries and private accountability agents” and “[p]articipat[e] in international and regional initiatives for data privacy protection”.⁶¹

120 Moreover, despite the fact that the NPC was only recently established, the NPC is now an accredited member of the International Conference of Data Protection and Privacy Commissioners (“ICDPPC”). It was during the 38th ICDPPC, held in Marrakech on

58 “(n) Ensure proper and effective coordination with data privacy regulators in other countries and private accountability agents, participate in international and regional initiatives for data privacy protection[.]”

59 “(o) Negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws[.]”

60 Republic Act No 10173 s 7.

61 Implementing Rules and Regulations of Republic Act No 10173 ss 8(a)(6) and 8(a)(7).

17 October 2016, when the Executive Committee of the ICDPPC recommended the accreditation of the Philippines.

ii *Enforcement of cross-border transfer restrictions*

121 The DPA does not contain any provision that specifically deals with a breach of provisions on international data transfers or data localisation. However, any covered entity which violates any of the provisions in the Act, regardless of whether the transfer of data is local or international, may be administratively, civilly or criminally liable.

122 Under the DPA IRR, the NPC may use its enforcement powers when it seeks to implement the provisions of the aforementioned law. Pursuant to its enforcement powers, the NPC may, among other things, issue compliance or enforcement orders, award indemnity, issue cease and desist orders, recommend to the DOJ the prosecution of data privacy crimes, compel or petition any entity to abide by its orders, and to impose administrative fines. While it is not provided for in the DPA nor in the DPA IRR, the NPC has a Legal and Enforcement Office that deals with data privacy complaints and enforcement matters.

123 The NPC is a regulatory and quasi-judicial body. Not only is it mandated to act on complaints lodged before it, the NPC may also, on its own initiative, investigate the circumstances surrounding serious privacy violations. It is empowered to use its enforcement powers to order the co-operation of the personal information controller or other persons with its investigation, or to compel the same to take appropriate action.⁶²

124 Parenthetically, while the NPC has the right to conduct an investigation and render a decision with respect to an investigation or a complaint, any personal information that comes to the knowledge and possession of the Commission shall remain confidential.⁶³ Notwithstanding this, however, “any personal data submitted may be transferred to parties who will be contacted during the handling of the

62 NPC Circular 16-04 – Rules of Procedure s 23.

63 NPC Circular 16-04 – Rules of Procedure s 31.

case and may be disclosed to agencies who are authorized to receive information relating to law enforcement, prosecution or review of the Commission's decisions".⁶⁴

125 As of this writing, the NPC has yet to take any action against a controller with respect to cross-border transfers of information.

iii *International enforcement by PEAs*

126 Aside from the ICDPPC, the NPC does not yet belong to any regional or international networks that may adopt guidelines or develop enforcement actions jointly. However, the DPA does give the NPC sufficient powers to co-ordinate, negotiate and contract with other PEAs for the proper implementation of their respective privacy laws.

127 The DPA, despite being the baseline privacy regulation in the Philippines, does not provide for a mechanism with regard to transfer of complaints to PEAs in other jurisdictions. Neither does it specifically authorise the NPC to disclose to PEAs in other jurisdictions information obtained during the course of an investigation or to assist other PEAs in cross-border investigations. However, all these matters may be reasonably presumed to have been subsumed under section 7 of the DPA, which mandates the NPC to, among other things, co-ordinate with other PEAs.

128 It should also be noted that despite the NPC's obligation to maintain the confidentiality of any personal information it comes across during its investigations, the NPC is permitted to disclose such information to "parties who will be contacted during the handling of the case and may be disclosed to agencies who are authorized to receive information relating to law enforcement, prosecution or review of the Commission's decisions".⁶⁵

129 As of this writing, the NPC has yet to publish an enforcement policy on either data transfers or data localisation requirements.

64 NPC Circular 16-04 – Rules of Procedure s 31.

65 NPC Circular 16-04 – Rules of Procedure s 31.

130 Given that the NPC was only established in 2016, it has yet to participate in the Global Privacy Enforcement Network (“GPEN”), the GPEN Alert, the ASEAN CPEA, the ICDPPC Enforcement Arrangement, and the Unsolicited Communication Enforcement Network (“UCENET”). Moreover, it does not yet perform an enforcement role under the APEC CBPR system.

131 Finally, the NPC has yet to enter into any bilateral agreements with other PEAs for the enforcement of their respective privacy laws. Neither has it been involved in any multi-country effort involving data privacy. Again, given the relatively recent establishment of the NPC, it has yet to undertake a joint investigation with another PEA or to provide assistance to an investigation being undertaken by a PEA from another country. Finally, the NPC has not had the opportunity to transfer a complaint to a PEA in another country, nor has it been on the receiving end of a foreign complaint.

Jurisdictional Report

SINGAPORE

Reporter: **Ken Chia***

Principal, Baker McKenzie Wong & Leow

A BACKGROUND INFORMATION

1 The Singapore government's position is that international data flows are essential to Singapore's economy and that high data protection standards are essential to maintain Singapore's position as a trusted data hub.¹

2 To support international data flows, Singapore announced in 2017 that it will participate in the Asia-Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules ("CBPR") system and the APEC Privacy Recognition for Processors ("PRP") system, and approval was granted by the Joint Oversight Panel ("JOP") to this initiative on 20 February 2018. Further, the new Data Protection Trustmark is anticipated to support certification of key products and services like mobile apps and online services in addition to verifying an organisation's compliance generally.

* The reporter gratefully acknowledges the contributions of the Personal Data Protection Commission of Singapore to the responses to the questionnaire on the basis of which this report was drafted. All errors are this reporter's own.

1 See the "Report of the Committee on the Future Economy" (February 2017) at para 78b which speaks of the need to "enhance our regional trade architecture to support digital businesses and data flows, such as developing mutual recognition of data protection standards". There are also other press releases on this topic at <<https://www.gov.sg/microsites/future-economy/press-room/news/content/leverage-the-digital-economy>> (accessed 10 April 2018).

3 In July 2017, the Minister for Communications and Information said:²

In the digital economy, data flows do not happen solely within the confines of Singapore's borders but take place internationally. In 2014, cross-border data flows accounted for almost US\$3 trillion of global GDP. The direct value added to Singapore's GDP of data connectivity in trade is estimated at around 40%. These numbers will only increase in the future. As they do, the international community will demand higher cross-border data protection standards so that customers and businesses overseas can exchange data with Singapore with the assurance that we will use the data responsibly.

I am therefore pleased to announce that Singapore has – this week – submitted our Notice of Intent to participate in the APEC Cross-Border Privacy Rules System and the APEC Privacy Recognition for Processors System – or the APEC CBPR and PRP – and will align our DP Trustmark standards with these. The APEC CBPR system harmonises data standards across participating economies, allowing businesses to share data responsibly across borders more seamlessly. Businesses can enjoy more clarity, save on the cost of ensuring compliance with multiple standards across different economies, and retain consumer confidence in the responsible handling of their data. Companies that obtain our DP Trustmark standards will concurrently be certified under the APEC CBPR.

4 Singapore's Infocomm Media 2025 Plan envisions a Singapore transformed for the better by infocomm media. It seeks to create a globally competitive ecosystem that enables Singapore's "Smart Nation" vision, effects economic and social transformation and creates enriching and compelling content. The plan supports industry players and solutions becoming globally competitive and includes boosting infrastructure to make Singapore a "Digital Harbour" with a digital corridor to the region.

5 Singapore is positioning itself as an international data and analytics hub,³ and as a hub it needs to ensure that data can flow across borders

2 Speech by Dr Yaacob Ibrahim, Minister for Communications and Information, at the Personal Data Protection Seminar 2017 at Sands Expo and Convention Centre on 27 July 2017.

3 Infocomm Media Development Authority, –"Data & Analytics, a Key Driver of Competitiveness and Growth" (6 October 2017).

both ways, hence participation in schemes like the APEC CBPR will be increasingly important.

6 The challenges to local and foreign businesses operating in this regional market are the different privacy laws and controls on cross-border data flows which apply. Data localisation laws in China, Indonesia and Vietnam are another trade barrier. These differences in the extreme result in businesses being unable to easily transfer data out of such countries, being forced to use potentially less secure local data centres, and at the very least having to deal with different classifications of sensitive data which impact on what they can collect and transfer. Where employee data is concerned, businesses face issues conducting cross-border investigations and using shared services.

7 Compliance with cross-border data controls do have some impact on local businesses or foreign businesses which operate in this jurisdiction or overseas as they will generally need to enter into data transfer agreements to comply with the Personal Data Protection Act 2012⁴ (“PDPA”) and other relevant laws, given that there are no real alternatives yet (*eg*, via adequacy decisions, CBPR, *etc*).

B LEGAL FRAMEWORK OF INTERNATIONAL DATA TRANSFERS IN SINGAPORE

8 The driving force behind the passing of a data protection reform in Singapore has neither been the human-rights approach favoured in the European Union (“EU”), nor the “threat-technology-structure mix that has driven reform in the US”, but “the imperative of globalisation and the need to adopt standards that will afford trust in national institutions and seamless integration into global networks”.⁵

9 Indeed, Singapore has not ratified or signed the International Covenant on Civil and Political Rights (“ICCPR”), nor ratified or signed the Optional Protocol to the International Covenant on Civil and

4 Act 26 of 2012.

5 Simon Chesterman, *Data Protection Law in Singapore* (Academy Publishing, 2014) at p 14.

Political Rights. However, it is a Member State to the Association of Southeast Asian Nations (“ASEAN”) Human Rights Declaration,⁶ whose Article 21 declares that: “Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attacks upon that person’s honour and reputation. Every person has the right to the protection of the law against such interference or attacks.”

10 Article 9(1) of the Constitution of the Republic of Singapore⁷ further provides that “[n]o person shall be deprived of his life or personal liberty save in accordance with law”, wording identical to Article 21 of the Constitution of India. To date, there has not been any case in Singapore similar to the Indian Supreme Court case of *Justice K S Puttaswamy v Union of India*, which held that Article 21 protects the right to privacy “as an intrinsic part of the right to life and personal liberty” in India.

11 Undeniably, the primary impetus for adopting a data protection law in Singapore was economic, following “the imperative of globalisation and the need to adopt standards that will afford trust in national institutions and seamless integration into global networks”.⁸

12 From the outset, therefore, the regulation of international data transfers has been a core factor in the passing of a data protection law in Singapore.

i *International data transfers in national data protection legislation – Overview*

13 Since 2012, next to “a bundle of common law rights and statutory torts which collectively form an incipient branch of law on privacy in

6 ASEAN Human Rights Declaration, adopted at Phnom Penh, Cambodia, on 18 November 2012.

7 1999 Rev Ed.

8 Simon Chesterman, *Data Protection Law in Singapore* (Academy Publishing, 2014) at p 14.

Singapore”, the PDPA is the baseline data protection legislation in force in Singapore.⁹

14 The Personal Data Protection Commission (“PDPC”), the privacy enforcement authority (“PEA”) for Singapore, plays a key role in the implementation of the PDPA, including the rules on international data transfers from Singapore.

15 The PDPA contains the data protection obligations applicable to the private sector generally, as the PDPA does not apply to the Government. Specifically, section 4(1)(c) of the PDPA states that “parts III to VI shall not impose any obligation on any public agency or an organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data”.

16 The so-called “Transfer Limitation Obligation” is found in section 26 of the PDPA which provides that:

- (1) An organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act.
- (2) The PDPC may, on the application of any organisation, by notice in writing exempt the organisation from any requirement prescribed pursuant to subsection (1) in respect of any transfer of personal data by that organisation.
- (3) An exemption under subsection (2) —
 - (a) may be granted subject to such conditions as the PDPC may specify in writing; and
 - (b) need not be published in the Gazette and may be revoked at any time by the PDPC.
- (4) The PDPC may at any time add to, vary or revoke any condition imposed under this section.

9 Keynote Speech by Mr Yeong Zee Kin, Deputy Commissioner of the Personal Data Protection Commission, at the 39th International Conference of Data Protection and Privacy Commissioners in Hong Kong (28 September 2017).

17 Regulations and subsidiary legislation have been passed under the PDPA, among which the Personal Data Protection Regulations 2014¹⁰ (“PDP Regulations”) and the Personal Data Protection (Enforcement) Regulations 2014¹¹ (“PDP Regulations (Enforcement)”), which are specifically relevant to this report.

18 Part III of the PDP Regulations sets out the requirements for transfer of personal data outside Singapore and what constitutes “legally enforceable obligations” that provide a standard of protection that is at least comparable to the protection under the PDPA to personal data transferred overseas (section 26(1) of the PDPA). These measures include the use of contractual agreements to ensure that the recipient overseas is bound by legally binding obligations to provide a comparable standard of protection.

19 The PDPC’s “Advisory Guidelines on Key Concepts in the Personal Data Protection Act” (“PDPC Guidelines on Key Concepts”) contains important guidance on the transfer limitation obligation in Chapter 19 (see below). The PDPC’s guides and resources also refer to international data transfers as a factor that organisations must consider in facing their data protection responsibilities, for instance when conducting a data protection impact assessment (“DPIA”).

20 Furthermore, the PDPC has a role in assessing and imposing sanctions on organisations for breach of the transfer limitation obligation (see below).

ii *International data transfers in banking sector*

21 The PDPA does not supersede existing statutes, such as the Banking Act¹² and Insurance Act¹³ applicable to banks and insurers in Singapore, but will work in conjunction with them and the common law.

10 S 362/2014.

11 S 455/2014.

12 Cap 19, 2008 Rev Ed.

13 Cap 142, 2002 Rev Ed.

22 A specific data protection regime applies to cross-border transfer of data in the banking industry. This regime is enforced by the Monetary Authority of Singapore (“MAS”), which regulates financial institutions and enforces the banking secrecy obligations under the Banking Act.

23 Banks in Singapore are required to ensure that the confidentiality of “customer information” (of which “personal data” seem to be considered a subset) is protected in all outsourcing arrangements to service providers pursuant to the “Banking Secrecy Outsourcing Conditions” issued by MAS (“MAS Notice 634”) and to demonstrate their compliance with the MAS “Guidelines on Outsourcing” (“MAS Guidelines”).

24 Paragraph 5.10 of the MAS Guidelines specifically deals with “Outsourcing Outside Singapore”. As a rule, the use of data centres outside of Singapore is permitted. However, institutions should, if services are provided from outside of Singapore, take into account, on a continuous basis, the applicable government policies, political, social and economic conditions, legal and regulatory developments and the institution’s ability to effectively monitor the service provider (paragraph 5.10.1).

25 Moreover, paragraph 5.10.2 sets higher standards for service providers which enter into a “material outsourcing arrangement”. Such an arrangement, as provided in paragraph 3.1 of the MAS Guidelines, means:

... an outsourcing arrangement –

- (a) which, in the event of a service failure or security breach, has the potential to either materially impact an institution’s –
 - (i) business operations, reputation or profitability; or
 - (ii) ability to manage risk and comply with applicable laws and regulations, or
- (b) which involves customer information and, in the event of any unauthorised access or disclosure, loss or theft of customer information [which is defined broadly], may have a material impact on an institution’s customers.

26 In consideration of the specific risks that may adversely affect the institution that has engaged a service provider in a foreign country, the MAS Guidelines require stricter standards by providing that: “Material

outsourcing arrangements with service providers located outside Singapore should be conducted in a manner so as not to hinder MAS' efforts to supervise the Singapore business activities of the institution (ie, from its books, accounts and documents) in a timely manner ..."

27 This means, in principle, that the bank should enter into outsourcing arrangements "only with service providers operating in jurisdictions that generally uphold confidentiality clauses and agreements" (paragraph 5.10.2(a)).

28 The bank should also not enter into outsourcing arrangements with service providers in "jurisdictions where prompt access to information by MAS or agents appointed by MAS to act on its behalf, at the service provider, may be impeded by legal or administrative restrictions". The bank must at least commit to retrieve information readily from the service provider should MAS request for such information. The bank should also confirm in writing to MAS that the bank has provided, in its outsourcing agreements, for MAS to have the right to inspect the service provider, as well as the right of access to the bank and service provider's information, reports and findings related to the outsourcing arrangement, as set out in the MAS Guidelines (paragraph 5.10.2(b)).

29 Finally, the bank "should notify MAS if any overseas authority were to seek access to its customer information or if a situation were to arise where the rights of access of the institution and MAS ... have been restricted or denied" (paragraph 5.10.2(c)).

30 There is no publicly available information on the level of enforcement of MAS Notice 634 or the MAS Guidelines.

31 As the PDPA is intended to be a baseline law (*ie*, other written laws prevail to the extent that any provision of Parts III to VI of the PDPA are inconsistent with the provisions of that other written law),¹⁴ written laws like MAS Notice 634 will prevail over the PDP Regulations to the extent they may be inconsistent.

14 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(6)(b).

iii *Impact of regional data protection frameworks*

32 Global and regional standards are important drivers of legal change in data protection in Singapore.

33 As Mr Leong Keng Thai, Chairman of the PDPC, said in 2015: “It is important for Singapore to keep abreast with international developments for our policies to stay relevant. This is fundamental in positioning Singapore as a trusted hub for data management and processing activities in this new digital age”.¹⁵ In accordance with that aim, Singapore has fully engaged in regional forums of co-operation, in Asia and beyond, and strongly supports broad regional frameworks that countries could agree on for the regulation of cross-border transfers of data.

34 Singapore being an APEC Member economy, the PDPC has opted to participate in the APEC Cross-border Privacy Enforcement Arrangement (“CPEA”). As mentioned in the introduction, Singapore has also lodged a Notice of Intent to participate in the APEC CBPR and PRP systems¹⁶ in July 2017.

35 Singapore is a member of the ASEAN Economic Community (“AEC”), and has reviewed the PDPA to ensure consistency with the ASEAN Framework on Personal Data Protection adopted in July 2016.

36 Out of the same concern for international consistency, the PDPC has extensively referred to the legislation of third countries (*eg*, Korea, Australia, the UK, the EU, Canada, New Zealand and the US) to propose amendments to the PDPA (*eg*, mandatory breach notification, notification of purpose and legal or business purpose as alternative bases to consent for collecting, using and disclosing personal data).¹⁷

15 Opening address at the Data Privacy Asia Conference (25 August 2015).

16 Speech by Dr Yaacob Ibrahim, Minister for Communications and Information, at the Personal Data Protection Seminar 2017, at Sands Expo and Convention Centre on 27 July 2017.

17 See Personal Data Protection Commission, “Public Consultation for Approaches to Managing Personal Data in the Digital Economy” (27 July 2017).

37 Furthermore, as Singapore is a hub for many businesses serving regional and global markets, it is likely that the extraterritorial effects of the European General Data Protection Regulation (“GDPR”) will have a significant impact on the data processing activities of businesses in the jurisdiction. To anticipate the consequences of these effects, the PDPC has recently issued a factsheet on the GDPR for organisations to highlight key requirements of the GDPR to organisations in Singapore.

iv *International data flows and free trade agreements*

38 Singapore has 21 implemented free trade agreements (“FTAs”) with 32 trading partners,¹⁸ which deal with data protection issues in a variety of ways. In general, one might say that the provisions related to data protection and privacy in these FTAs are generally not specific enough to override the restrictions on cross-border data transfers in the national laws of the parties to the FTA, when they exist. Some examples are the EU-Singapore FTA (this was intended to be the template for other modern EU FTAs with the Asian region), Australia-Singapore FTA and Japan-Singapore FTA (these are FTAs with Singapore’s Asia-Pacific neighbours and potential Comprehensive and Progressive Agreement for Trans-Pacific Partnership (“CPTPP”) partners), and others with China and the Gulf Cooperation Council (“GCC”) which contain no references to data protection.

39 The first example is Singapore’s FTA with the EU (“EUSFTA”), which was signed in 2014 but is still awaiting ratification by all the EU Member States, whose Chapter 8 on “Services, Establishment and Electronic Commerce” addresses specific issues in relation to data protection.

40 Article 8.62 of the EUSFTA (“General Exceptions”) provides that:

[N]othing in this Chapter shall be construed to prevent the adoption or enforcement by either Party of measures:

...

18 See <<https://www.iesingapore.gov.sg/Trade-From-Singapore/International-Agreements/free-trade-agreements/Singapore-FTA>> (accessed 10 April 2018).

(e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter including those relating to:

...

(ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; ...

This rule is of course subject to the requirement “that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination against the other Party where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services”.¹⁹

41 Interestingly, similar wording has been retained in the Singapore-Australia FTA (“SAFTA”), signed on 13 October 2016, and the Japan-Singapore Economic Partnership Agreement (“JSEPA”) originally signed in 2002 and later revised in 2007 (Article 69 – “General Exceptions under Chapter 7” (“Trade in Services”)).

42 In Section F on “Electronic Commerce”, Article 8.57.4 of the EUSFTA also provides that: “The Parties agree that the development of electronic commerce must be fully compatible with international standards of data protection, in order to ensure the confidence of users of electronic commerce.”

19 It is likely that this precaution derives from the commitment made by the European Commission to the European Parliament and Council that “Rules on the processing of personal data are not negotiated in, or affected by, trade agreements” (Communication of the European Commission, “Trade for all – towards a more responsible trade and investment policy” (October 2015) at p 12), although “the existence on an FTA or ongoing negotiations ... with a given third country” are factors to be considered by the European Union for instance “when assessing with which third countries a dialogue on adequacy should be pursued” (Communication of the European Commission, “Exchanging and Protecting Personal Data in a Globalised World” (January 2017) at pp 7–8).

43 The EUSFTA also contains specific data protection provisions in its Sub-Section 6 on “Financial Services”. Article 8.54 on “Data Processing” states that:

1. Each Party shall, subject to appropriate safeguards on privacy and confidentiality, permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier.
2. Each Party shall adopt or maintain appropriate safeguards to protect privacy and personal data, including individual records and accounts, as long as these safeguards is not used to circumvent the provisions of this Agreement.

44 Article 9 of Understanding 3 of the EUSFTA on “Additional Customs-related Provisions” also provides that: “Personal data may be exchanged only where the Party which may receive them undertakes to protect such data in a manner that is considered adequate by the Party that may supply them.”

45 In contrast, the US-Singapore Joint Statement on Electronic Commerce²⁰ mentions personal data privacy protection only at a high level. Its Section 23 thus provides that:

Ensuring the effective protection of personal data on global information networks is necessary, as is the need to continue the free flow of information. Governments and businesses should consider consumers’ concern about their private information, as well as the needs of law enforcement. Since content, usage, and the method for collection of private information differ from industry to industry, means for data protection should be flexible. Governments should encourage the private sector to develop and implement enforcement mechanisms, including preparing guidelines and developing verification and recourse methodologies. Both Parties welcome on-going work to develop international guidelines as a useful basis for policy development in this area.

46 Similarly, Article 9.7 of the Turkey-Singapore FTA, which was signed in November 2015 and entered into force in October 2017, only covers personal data protection at a high level:

20 US-Singapore Joint Statement on Electronic Commerce (18 November 2002).

1. The Parties recognise the economic and social benefits of protecting the personal data of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce.
2. To this end, each Party shall adopt or maintain a domestic legal framework that provides for the protection of the personal data of users of electronic commerce.
3. The Parties shall publish information on the personal data protections it provides to users of electronic commerce, including:
 - (a) how individuals can pursue remedies; and
 - (b) how business can comply with any legal requirements.

47 By contrast, other FTAs like the China-Singapore FTA of 2008 or the GCC-Singapore FTA of 2013 make no reference to data protection at all. These are not surprising given that China and the GCC do not have comprehensive privacy laws in place yet.

C DATA LOCALISATION

48 There are no data localisation requirements which apply in Singapore.

D DEFAULT POSITION AND SCOPE OF TRANSFER LIMITATION OBLIGATION AND TERRITORIAL EFFECT OF PDPA

i Default position on data transfers in PDPA

49 Under section 26 of the PDPA, international data transfers are forbidden as a rule, with exceptions.

50 This rule has extraterritorial effect in that the organisation can be located outside of Singapore, and yet still be subject to the transfer limitation obligation. Under the PDPA, an organisation is defined as “any individual, company, association or body of persons, corporate or unincorporated, whether or not – (a) formed or recognised under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore”.

ii Scope of the transfer limitation obligation

a Nature of data covered by transfer limitation obligation

51 The data export restrictions apply to all personal data covered by the PDPA. This includes the personal data of all individuals, whether they have been collected within or outside Singapore, as the PDPA applies to inbound data transfers.²¹ The Act does not distinguish between the individuals concerned depending on their nationality or usual place of residence.

52 Business contact information (section 4(4)(b)) and personal data about deceased individuals (section 4(5)) are in-principle excluded from the scope of the PDPA.

53 Personal data that is publicly available in Singapore may also be freely transferred, in accordance with regulation 9 of the PDP Regulations. Section 2(1) of the PDPA defines “publicly available data” as “personal data that is generally available to the public, and includes personal data which can be observed by reasonably expected means at a location or an event – (a) at which the individual appears; and (b) that is open to the public”.

54 Regulation 9 further provides for an exception for “data in transit” which regulation 8 defines as:

... personal data transferred through Singapore in the course of onward transportation to a country or territory outside Singapore, without the personal data being accessed or used by, or disclosed to, any organisation (other than the transferring organisation or an employee of the transferring organisation acting in the course of the employee’s employment with the transferring organisation) while the personal data is in Singapore, except for the purpose of such transportation.

The PDPC’s “Advisory Guidelines on the Transfer Limitation Obligation” (paragraph 19.3(f)) gives an example of data in transit as

21 Personal Data Protection Commission, “Advisory Guidelines on Key Concepts in the Personal Data Protection Act” (Chapter 11).

“data from overseas passing through servers within Singapore enroute to its destination overseas”.

55 Anonymised data may fall outside the definition of personal data and hence be freely transferred overseas. Indeed, the chapter on “Anonymisation” in the PDPC’s “Advisory Guidelines on the Personal Data Protection Act for Selected Topics” states at paragraph 3.4 that “data that has been anonymised is not personal data, and the Data Protection Provisions in Parts III to VI of the PDPA do not apply to the collection, use or disclosure of such data”. The PDPC has released materials to further explain how anonymisation helps manage personal data protection risks.²²

56 The chapter further describes the considerations and conditions under which personal data may be anonymised and no longer considered personal data for the purposes of the PDPA. As a rule, if an organisation has access to other information that can re-identify the individuals (*eg*, the organisation holds the “key” to re-identification), the dataset will not be treated as anonymised and will continue to be considered as personal data to which the transfer limitation obligation will apply.

b Type of organisations covered by transfer limitation obligation

57 The PDPA distinguishes between “organisations” and “data intermediaries” generally but for the purposes of the transfer limitation obligation, the PDPA does not expressly prescribe different requirements for transfers to “controllers” as opposed to “processors”.

58 The PDPA does not exempt some categories of sectors or companies from the application of provisions in the Act, including provisions relating to cross-border data flows.

22 Personal Data Protection Commission, “Anonymisation: Managing Personal Data Protection Risk” (DPO Connect, November 2015).

E LEGAL BASIS AND MECHANISMS FOR DATA TRANSFERS

59 The combined application of section 26 of the PDPA, regulation 9 of the PDP Regulations and paragraph 19 of the PDPC Guidelines on Key Concepts provides a wide array of legal bases and mechanisms for transferring personal data to a country or territory outside Singapore.

60 Whatever the chosen basis or mechanism, the transferring organisation remains responsible to ensure that the personal data which will be transferred have been collected and used in compliance with Parts III to VI of the PDPA (regulation 9(1)(a) of the PDP Regulations).

61 The transferring organisation may rely on one out of different legal bases provided it meets the general requirement that it has taken “appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data in that country or territory outside Singapore (if any) is bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the Act” (regulation 9(1)(b) of the PDP Regulations).

62 According to the PDPA and regulations 9 and 10, “legally enforceable obligations” that provide such a “comparable level of protection” include obligations that can be imposed on the recipient by the local law of the country of destination, a contract, Binding Corporate Rules (“BCR”) or “any other legally binding instrument”. The requirements of section 26 of the PDPA may also be satisfied if the transferring organisation obtains the individual’s consent to that effect, or if it falls within the scope of narrowly defined exceptions.

63 These bases and mechanisms are studied below.

i *Individual decision by PDPC to exempt organisation from section 26(1) upon request*

64 While data transfers are not subject to a requirement of notification to, or approval by the PDPC, the Government or another public entity, the PDPC may, on the application of any organisation, “by notice in writing exempt the organisation from any requirement prescribed

pursuant to subsection 26(1) in respect of any transfer of personal data by that organisation, subject to such conditions as the Commission may specify in writing”. It may further “at any time add to, vary or revoke” any condition that may have been imposed under this section. In September 2017, the PDPC announced that it would create regulatory sandboxes on the basis of section 26(2) to exempt organisations from the transfer limitation obligation, upon request, and subject to specific criteria.²³

ii *“Adequacy findings” and white lists*

65 “Legally enforceable obligations” in the meaning of regulation 9 of the PDP Regulations include obligations imposed on the recipient under “any law”, which means that data transfers to jurisdictions that have laws establishing adequate or comparable data protection standards will be permitted. The PDPC has not yet issued any formal adequacy decisions to that effect, so the data exporter remains free to assess the level of protection awarded in the country of destination.

66 The PDPA does not list substantive standards (*eg*, ratification of an international data privacy instrument or existence of a PEA) to establish that the law of another jurisdiction establishes comparable data protection standards. However, the PDPC could issue advisory guidelines setting out the criteria for assessment. Under section 65 of the PDPA, the Minister for Communications and Information may also make such regulations “as may be necessary or expedient for carrying out the purposes and provisions of [the PDPA] and for prescribing anything that may be required or authorised to be prescribed by [the PDPA]”. This was the authority under which the PDP Regulations was issued.

67 The PDPA can accommodate decisions of “sectoral adequacy”, *ie*, the finding that comparable legal standards apply in one specific sector in the country of destination, as the Minister has considerable flexibility in what the transfer regulations could cover.

23 See Personal Data Protection Commission, “Data Sharing Arrangements” <<https://www.pdpc.gov.sg/legislation-and-guidelines/exemption-requests/data-sharing-arrangements/>> (accessed 10 April 2018).

68 Similarly, the PDPC could issue advisory guidelines or the Minister could issue new regulations to establish “white lists” of jurisdictions (inside or outside Asia) which have adequate or comparable data protection standards. It is equally conceivable that a “black list” of jurisdictions (inside or outside Asia) which do not have adequate or comparable data protection standards could be issued.

69 There is no prescribed procedure to be followed and the PDPA can accommodate a principle of reciprocity or the mutual recognition of such lists. In this respect, it is worth noting that the Committee on the Future Economy (“CFE”) has recommended that Singapore would “need to enhance [its] regional trade architecture to support digital businesses and data flows, such as developing mutual recognition of data protection standards”, in the context of continuing to work with “like-minded partners to pursue the liberalisation of trade and investment” and many economic players who are committed to open trade.²⁴

70 A cost/benefit analysis of “adequacy” decisions and white/black lists has not to our knowledge been done yet in Singapore. There is probably enough data to potentially complete such an analysis, but only for the major jurisdictions which Singapore deals with.

iii *Consent as exception to existence of privacy safeguards overseas*

71 While the transfer limitation obligation in section 26 of the PDPA is independent of the consent obligation in its section 13, consent of the individual can be used to satisfy the requirement of section 26.

72 However, by application of regulation 9(4) of the PDP Regulations, that condition will not be deemed satisfied if:

- (a) the individual was not, before giving his consent, given a reasonable summary in writing of the extent to which the personal data to be

24 “Report of the Committee on the Future Economy” (February 2017) at para 78.

transferred to that country or territory will be protected to a standard comparable to the protection under the Act;

(b) the transferring organisation required the individual to consent to the transfer as a condition of providing a product or service, unless the transfer is reasonably necessary to provide the product or service to the individual; or

(c) the transferring organisation obtained or attempted to obtain the individual's consent for the transfer by providing false or misleading information about the transfer, or by using other deceptive or misleading practices.

73 It is important to note that under regulation 9(4)(a) specifically, consent cannot be used to waive the requirement of existing privacy safeguards in the country of destination since consent can only be used by providing the individual with “a reasonable summary in writing of the extent to which the personal data to be transferred to that country or territory will be protected to a standard comparable to the protection under the Act”.

74 Practically, save for specifically identified transfers to a particular organisation or data intermediary, it is difficult to provide a “reasonable summary in writing” in sufficient detail to satisfy the requirements in regulation 9(4)(a), given that each recipient will likely have implemented different ways of protecting the personal data. As a result, most organisations will use the alternative written data transfer agreement route.

75 Paragraph 19.4 of the PDPC Guidelines on Key Concepts provides examples to illustrate certain situations in which organisations may transfer personal data overseas in compliance with the transfer limitation obligation:

Cedric is a client of Organisation GHI. Organisation GHI notifies Cedric in writing that it is adopting a cloud-based solution to store and analyse its client data, which includes personal data such as clients' identification details, address, contact details and income range, and asks for Cedric's consent to move his client data to the cloud-based solution. Organisation GHI also provides Cedric with a written summary of the extent to which Cedric's personal data will be protected to a standard comparable to that under the PDPA, in the countries and territories that it will be transferred to. Should Cedric provide his consent, Organisation

GHI would be able to transfer his personal data in compliance with the Transfer Limitation Obligation.

iv *One-off transfers based on regulation 9(3)*

76 Other legal bases under the PDP Regulations for international data transfers are as follows:

- (a) the transfer of the personal data to the recipient is necessary for the performance of a contract between the individual and the transferring organisation, or to do anything at the individual's request with a view to the individual entering into a contract with the transferring organisation;
- (b) the transfer of the personal data to the recipient is necessary for the conclusion or performance of a contract between the transferring organisation and a third party which is entered into at the individual's request; and
- (c) the transfer of the personal data to the recipient is necessary for the conclusion or performance of a contract between the transferring organisation and a third party if a reasonable person would consider the contract to be in the individual's interest.

77 Under the condition that "the transferring organisation has taken reasonable steps to ensure that the personal data so transferred will not be used or disclosed by the recipient for any other purpose", the transfer of the personal data to the recipient is further possible when it is necessary:

- (a) in the interest of the individual, "if consent for its use cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent";
- (b) to respond to an emergency that threatens the life, health or safety of the individual or another individual;
- (c) in the national interest; or
- (d) to contact the next of kin or a friend of any injured, ill or deceased individual.

78 Chapter 19 of the PDPC Guidelines on Key Concepts can be referred to for further information.

v *Contracts*

79 Absent an official adequacy decision from the PDPC, and since relying on the “consent plus reasonable summary” mechanism (see above) is not practical, most organisations in Singapore would use the data transfer agreement mechanism to transfer data outside Singapore, although they could also rely on other grounds (*eg*, because there is an intra-group BCR in place already).

80 Moreover, the local data exporter may remain liable if there is a breach by the data importer overseas (where the data importer is a data intermediary) as the PDPA provides in section 4(3) that: “An organisation shall have the same obligation under this Act in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself.”

81 The requirement does have an impact on the type of transfer mechanism that data exporters should use in Singapore, as data exporters will want to ensure that the data importer complies with the PDPA requirements by way of contract so it can take action against the data importer if necessary.

82 Paragraph 19.5 of the PDPC Guidelines on Key Concepts states that a transferring organisation should minimally set out protections with regard to the following:

- (a) for data intermediaries: protection and retention limitation; and
- (b) for organisations: purpose of collection, use and disclosure by recipient, accuracy, protection, retention limitation, policies on personal data protection, access and correction.

It is expected that organisations engaging such data intermediaries would generally have imposed obligations that ensure protection in the relevant areas in their processing contract.

83 On 20 July 2016, the PDPC published a “Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data”, which can be used in cross-border data transfer agreements. These clauses are not meant to be mandatory, however, and

can be varied by parties. The different sets of European Standard Contractual Clauses (“SCCs”) are also used in Asia, but usually with amendments to supplement the SCCs to cater for local requirements, for example, in Singapore additional clauses regarding the territories to which the personal data will be exported and compliance with the retention limitation obligation are required to be added.

84 In particular, the contract concluded between the data exporter and importer does not need to contain a third-party beneficiary clause to the benefit of the individual whose data are transferred. Singapore has a Contracts (Rights of Third Parties) Act²⁵ which enables third-party beneficiaries to sue on a contract to which they are not a party. However, the Act is frequently excluded, and it is not clear if the individual (or better still the PDPC) would be treated as an intended beneficiary of the data protection provisions in the data transfer agreement.

85 It is suggested that the joint adoption of standard clauses by several Asian countries would be useful to categories of companies such as small and medium-sized enterprises who would not otherwise have the benefit of legal advice.

vi CBPR

86 As mentioned earlier, Singapore has announced that it will participate in the APEC CBPR and PRP systems in July 2017. With approval from the APEC Joint Oversight Panel, on 20 February 2018, Singapore has become the sixth APEC economy to participate in the CBPR system alongside the US, Mexico, Canada, Japan and the Republic of Korea, and the second APEC economy to participate in the PRP system alongside the US. No changes to the law have yet been made to facilitate such participation, and no accountability agent (“AA”) has yet been identified or appointed for Singapore. However, the PDPC has announced that it is working on the certification scheme and companies can start applying for the CBPR and PRP systems certification in 2019.

25 Cap 53B, 2002 Rev Ed.

87 Several multinational corporations have expressed an interest in being CBPR-certified but as Singapore has not yet fully joined the CBPR and PRP systems, no companies have been CBPR or PRP-certified in Singapore.

88 The PDPA does not specifically address whether the implementation of different types of certification depending on the size and profile of companies is possible.

vii *Certification, trustmarks and privacy seals*

89 As mentioned above, in July 2017, Singapore announced plans to introduce a Data Protection Trustmark certification scheme by end 2018, the development of which was entrusted to the PDPC. The new Data Protection Trustmark is anticipated to support certification of enterprise-wide or key products and services like mobile apps and online services in addition to verifying an organisation's compliance generally.

90 Together with a series of resources, the "DP Trustmark" certification scheme aims "at encouraging organisations to be transparent and accountable in their data protection measures ... The resources will also help to facilitate locally-based organisations' ability to exchange information across borders, while attracting more businesses to conduct data innovation activities in Singapore".²⁶ The adoption of a DP Trustmark participates in the objective of building a "Trusted Data Ecosystem to Support Singapore's Digital Economy".

91 No details of how the DP Trustmark will be implemented are publicly available yet, except for the fact that the DP Trustmark standards will be aligned with the APEC CBPR PRP systems.²⁷

26 Speech by Dr Yaacob Ibrahim, Minister for Communications and Information, at the Personal Data Protection Seminar 2017, at Sands Expo and Convention Centre on 27 July 2017.

27 Speech by Dr Yaacob Ibrahim, Minister for Communications and Information, at the Personal Data Protection Seminar 2017, at Sands Expo and Convention Centre on 27 July 2017.

92 Certification mechanisms, privacy seals and trustmarks delivered in a third country could be considered as a valid means for a data exporter to demonstrate compliance with local cross-border data controls, since it could help the data exporter to demonstrate that “the recipient of the personal data in that country or territory outside Singapore (if any) is bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the Act”.

93 The PDPA does not currently expressly provide for a mechanism of mutual recognition of trustmarks or privacy seals delivered in another jurisdiction.

viii BCR

94 The PDP Regulations recognise the use of BCR for intra-group transfers (it may only be used for recipients that are related to the transferring organisation).

95 The PDP Regulations also recognise the use of “any other legally binding instrument”, but no other instrument than the ones mentioned above has yet been listed.

F INTERNATIONAL CO-OPERATION BETWEEN PDPC AND OTHER PRIVACY ENFORCEMENT AUTHORITIES

i *Co-operation with foreign counterparts in areas other than enforcement*

96 Section 10 of the PDPA allows the PDPC to enter into co-operation agreements with foreign data protection bodies to “facilitat[e] co-operation between the PDPC and another regulatory authority in the performance of their respective functions in so far as those functions relate to data protection”.

97 Besides plans to participate in the APEC CBPR and PRP systems to facilitate cross-border data flows, Singapore is also exploring other avenues of bilateral or multilateral co-operation with foreign counterparts in the area of data protection, such as free trade negotiations, and mutual

recognition of data protection regimes between Singapore and its key trade and economic partners.

ii *Enforcement of cross-border restrictions*

98 Under section 29(1) of the PDPA, the PDPC may, if it is satisfied that an organisation is not complying with any provision in Parts III to VI of the PDPA (section 26 relating to transfer of personal data outside Singapore falls within Part VI of the Act), give the organisation such directions as it thinks fit in the circumstances to ensure compliance with that provision, including directions:

- (a) to stop collecting, using or disclosing personal data in contravention of this Act;
- (b) to destroy personal data collected in contravention of this Act;
- (c) to comply with any direction of the Commission under section 28(2);
- (d) to pay a financial penalty of such amount not exceeding \$1 million as the Commission thinks fit.

99 The PDPC has the power to investigate and issue directions under section 29 to ensure compliance with the PDPA. In that regard, the PDPC has a direct role in assessing and imposing sanctions for breach.

100 The PDPC's "Advisory Guidelines on Enforcement of the Data Protection Provisions" does not specifically address the enforcement of the transfer limitation obligation. However, as a rule, Singapore's regime generally allows organisations the flexibility to decide how they wish to comply with the PDPA. It generally only takes enforcement action when the organisation is unable to satisfactorily resolve issues with the affected individuals, or where many individuals may be affected by an organisation's contravention of the data protection provisions, or where an organisation contravened the data protection provisions intentionally or negligently, or it did not have the necessary policies, procedures and processes in place to ensure its compliance with the data protection provisions.²⁸

28 See Personal Data Protection Commission, "Advisory Guidelines on Enforcement of the Data Protection Provisions" at para 2.

101 The PDPC has not yet published any infringement decisions relating to a breach of the transfer limitation obligation based on the conditions in which local data had been transferred to another jurisdiction.

102 Under section 31(1) of the PDPA, an organisation or individual aggrieved by any direction made by the PDPC may, within 28 days after the issue of the direction or decision concerned, make a written application to the PDPC to reconsider the direction or decision.

iii *Participation in international enforcement networks*

103 The PDPC participates in international enforcement networks such as the APEC CPEA and Global Privacy Enforcement Network (“GPEN”) as part of its efforts to co-ordinate and share information and practices relating to data protection enforcement.

104 The PDPC joined as a member of the GPEN in October 2014. It has participated in the GPEN Sweep 2016 and 2017 and will likely selectively expand its involvement in such co-ordinated efforts.

105 The PDPC has not submitted its application to be an accredited member of the International Conference of Data Protection and Privacy Commissioners (“ICDPPC”) and it is also not a participant of the ICDPPC Enforcement Cooperation Arrangement either. However, the PDPC was an observer of the ICDPPC between 2013 and 2017, and its parent authority, the Infocomm Media Development Authority (formerly known as the Infocomm Development Authority of Singapore) was also an observer between 2014 and 2016.

iv *International co-operation agreements*

106 Section 10 of the PDPA allows the PDPC to enter into co-operation agreements with foreign data protection bodies in the performance of their respective functions relating to data protection, as mentioned above, but also to “avoid duplication of activities by the Commission and another regulatory body, being activities involving the enforcement of data protection laws”.

107 Based on section 10(2), such agreements may include provisions:

- (a) to enable the Commission and the other regulatory authority to furnish to each other information in their respective possession if the information is required by the other for the purpose of performance by it of any of its functions;
- (b) to provide such other assistance to each other as will facilitate the performance by the other of any of its functions; and
- (c) to enable the Commission and the other regulatory authority to forbear to perform any of their respective functions in relation to a matter in circumstances where it is satisfied that the other is performing functions in relation to that matter.

108 Furthermore, section 10(3) of the PDPA provides that the PDPC shall not furnish any information to a foreign data protection body pursuant to a co-operation agreement unless it requires of, and obtains from, that body an undertaking in writing by it that it will comply with terms specified in that requirement, including terms that correspond to the provisions of any written law concerning the disclosure of that information by the PDPC.

109 When an international co-operation agreement has been concluded based on section 10 of the PDPA, the PDPC is then authorised to disclose any information “necessary to comply with this agreement” (section 59), which may include information obtained in investigations as well as assistance in cross-border investigations.

110 However, three conditions must be satisfied to that effect (section 59(6) of the PDPA):

- (a) that the information or documents requested by the foreign country are in the possession of the Commission;
- (b) that unless the Government otherwise allows, the foreign country undertakes to keep the information given confidential at all times; and
- (c) that the disclosure of the information is not likely to be contrary to the public interest.

111 Under section 10(4) of the PDPA, the PDPC may also give an undertaking to a foreign data protection body that it will comply with terms specified in a requirement made of the PDPC by the foreign data protection body to give such an undertaking where:

- (a) those terms correspond to the provisions of any law in force in the country or territory in which the foreign data protection body is established, being provisions which concern the disclosure by the foreign data protection body of the information referred to in paragraph (b); and
- (b) compliance with the requirement is a condition imposed by the foreign data protection body for furnishing information in its possession to the Commission pursuant to a co-operation agreement.

112 To date, the PDPC does not yet have any bilateral or multilateral arrangements with the PEAs of other jurisdictions to co-operate in the implementation of privacy laws.

v *Participation in international forums and thought leadership*

113 The PDPC actively participates in international data privacy forums and meetings such as the Asia Privacy Bridge Forum to shape discussions and develop solutions to data protection regulations and issues such as cross-border data flows. The PDPC regularly shares its experience on preparing for the APEC CBPR and PRP systems through APEC-hosted and think-tank initiated workshops.

Jurisdictional Report

SOUTH KOREA

Reporter: **Kwang Bae Park**
Partner, Lee & Ko

A INTRODUCTION

1 Korea is known to have one of the strictest data protection regulatory regimes in the world.

2 Under the Constitution of Korea, the right to privacy is enshrined in the constitution as a fundamental right, and the right to control one's personal information is regarded as deriving from this fundamental right.

i *Overlapping statutory protections in Korean law*

3 Already in 1994, Korea regulated the collection and use of personal information in the public sector by enacting the Act on the Protection of Personal Information Maintained by Public Institutions. In 1999, the regulation was extended to the private sector, especially for communications and online services, with the enactment of the Act on Promotion of Information Communication Network Usage. The name of that last Act was changed in 2001 by the Act on Promotion of Information Communication Network Usage and Information Protection ("Network Act"), still in force today, and amended frequently to reflect the changes in the information communication environments in Korea until 2017.¹ Due to the increasing need to regulate personal information in the offline sector as well, the scope of the Network Act was progressively extended to the offline processing of personal information by department stores, travel agencies, *etc.* These provisions

1 See KLII, "Recent Amendments to the Network Act" <http://www.koreanlii.or.kr/w/index.php/Recent_amendments_to_the_Network_Act> (accessed 10 April 2018).

applicable to the offline world were superseded by the Personal Information Protection Act (“PIPA”) in 2011.

4 The PIPA is Korea’s omnibus data protection law. The Act broadly regulates all aspects of personal information processing. Specifically, it regulates various stages and aspects of personal information processing throughout the lifecycle of personal information, *ie*, from collection until destruction, and various uses of personal information by a data handler.² The PIPA further provides key definitions, such as the concept of “personal information”, which is key to the regulation of international data transfers under Korean law (see further down).

5 The PIPA was designed as a comprehensive Act regulating the processing of personal information in both the public and private sectors, with combined elements from previous statutes such as the Act on the Protection of Personal Information Maintained by Public Institutions (replaced by the PIPA) and the Network Act.

6 Several sector-specific laws regulate the processing of personal information in specific industries or information on top of the PIPA. These laws will generally take precedence over the PIPA when they are applicable. In the financial sector, for instance, the Act on the Use and Protection of Credit Information (“Credit Information Act”) has established the legal framework for the regulation of personal credit information (including both personal and corporate credit information). Other laws regulate personal information in the medical sector, such as the Medical Service Act, which contains specific provisions on the protection of electronic health records, or the Protection and Use of Location Information (“Location Information Act”).

2 Under the Personal Information Protection Act, a data handler refers to a public agency, corporation, organisation, or individual that processes personal information on its own or through a third party in order to operate a personal information file for business purposes. In most cases, a data handler corresponds to a data controller under the EU Data Protection Directive 95/46/EC or the General Data Protection Regulation, and the relationship between a data controller and a data processor are similar under EU and Korean data protection laws. The terms “data handler”, “data controller”, and “controller” have thus been used interchangeably in this report, and the same applies to the terms “outsourced data processor”, “data processor” and “processor”.

7 Therefore, prior to carrying out any assessment under the data protection laws in Korea, one must determine whether a sector-specific law, in addition to the PIPA, will apply to the processing of the personal information at issue. Furthermore, another important aspect to consider is that different regulatory authorities may be responsible for enforcing sector-specific law.

8 Security requirements offer a good example of the consequences of the possible legal overlap. While the PIPA imposes general security requirements on data handlers, different security requirements will apply to online service providers under the Network Act, which are classically considered more important. Financial institutions are subject to the cybersecurity requirements under the Credit Information Act, as well as to sector-specific requirements under other legislation (such as the Bank Act, the Act on Insurance Business and the Electronic Financial Transaction Act) and the regulations of the Financial Services Commission. Other laws impose security requirements in specific areas, such as medical information systems used by medical institutions.

ii *Multiple privacy enforcement authorities in Korea*

9 Different authorities administer the application of privacy protections in Korea, and more specifically the application of the rules on international data transfers.

10 The Personal Information Protection Commission (“PIPC”) is responsible for shaping data protection policy while assessing the necessity of adopting or amending laws and administrative measures relating to the protection of personal information. Lee Hong-Sub is the current Chair of PIPC.

11 The Ministry of the Interior and Safety (“MOIS”) is responsible for enforcing the PIPA, including its international data transfer rules. The current Minister of the Interior and Safety is Kim Boo Kyum.

12 The Korean Communications Commission (“KCC”), currently chaired by Lee Hyo-seong, is responsible for enforcing and issuing formal interpretations on the Network Act, including its international data transfer rules.

13 The Korea Internet & Security Agency (“KISA”), currently chaired by President Kim Suck-hwan, is a sub-agency tasked with privacy protection as well as Internet security, including international data transfer matters (*eg*, data breach investigations and regular investigations of violations).

14 Both PIPC and KISA are accredited Members of the International Conference of Data Protection and Privacy Commissioners (“ICDPPC”), while MOIS is an observer to the Conference.

iii Large reliance on explicit opt-in consent

15 Generally, explicit opt-in consent of the data subject is required for the processing of personal information by governmental and private entities (with limited exceptions for private entities and wider exceptions for governments) to protect the data subject’s constitutional “right to informational self-determination” (see below). However, these requirements seem to operate as serious impediments to business activities or industries that rely on extensive processing of personal information, *eg*, online target marketing or the big data industry. As a result, these activities and industries are under-developed in Korea in comparison to the country’s well-established IT infrastructure. The role of self-regulatory industry groups is very limited as well.

16 Due to these circumstances, there has been considerable criticism from affected industries and practitioners regarding the strict regulation of the processing of personal information. Efforts were thus made to amend regulations to address such criticisms. However, these efforts have been hampered by the increasing frequency of mass data breach incidents since 2008,³ and through the active resistance of privacy advocating organisations, mainly non-profit organisations (“NGOs”).

17 Under Korean law, consent from the data subject is a key requirement for cross-border data transfers, irrespective of the implementation of data transfer mechanisms by the exporter and/or

3 See, for instance, Steve Ragan, “27 Million South Koreans Affected by Data Breach” *CSO* (25 August 2014).

importer. Based purely on this reporter's personal experience as a data privacy law specialist, data subjects in Korea generally do not object to the export of their data when they are notified and asked to consent to the use of their personal information for cross-border transfers.

iv *Recent focus on international data transfers*

18 Cross-border transfers of personal information did not attract any particular interest from data protection regulators in Korea until 2015, when Korea started to consider applying for a European Union ("EU") adequacy decision under the EU data protection regime. Until then, the activities of regulators and legislators had remained focused mostly on issues such as technical, managerial and physical measures to prevent the leakage and misuse of personal information, on guaranteeing and strengthening the rights of data subjects, and strengthening consent requirements.

19 However, interest in cross-border data transfers became more pronounced with the rapid change affecting the information technology ("IT") industry with the advent of cloud computing, the Internet of Things ("IoT") and big data. Significant developments are thus expected to take shape in the future as efforts to obtain the EU adequacy assessment and participation in the Cross-Border Privacy Rules ("CBPR") intensify. Amendments to the cross-border data transfer provisions of the Network Act that are currently being considered in the National Assembly of Korea are reportedly directly related to these efforts.

B PROTECTION OF PERSONAL INFORMATION IN KOREAN LEGAL SYSTEM

20 This report will mainly focus on the regulatory framework and issues related to the PIPA and the Network Act, which contain the most significant provisions for cross-border data transfers under Korean law. Beyond the statutory framework of data transfers, however, it is important to be aware of the strong privacy protections that have been read into the Constitution of Korea, and of the international

commitments of Korea in the area of data protection and privacy, which will be specifically considered in this section.

i *Constitutional protection of privacy*

21 The strictness of Korean data protection laws must be read in the wider context of the constitutional protections of privacy, and the very important role of the Judiciary in the implementation of these protections.

22 The Constitution of Korea includes several references to privacy.⁴ Notably, Article 10 provides that “[a]ll citizens shall be assured of human worth and dignity and have the right to pursue happiness”, and Article 17 provides that “[t]he privacy of the citizen shall not be breached”.

23 Several judicial decisions have read privacy or data protection principles into the Korean Constitution. In a landmark decision handed down on 26 May 2005,⁵ the Constitutional Court acknowledged for the first time that Korean citizens have a right to “self-determination of personal information”, a concept closely related to the idea of informational self-determination developed by the German Constitutional Court. The court wrote:

The right to control one’s own personal information is the right of the subject of the information to personally decide when, to whom or by whom, and to what extent his or her information will be disclosed or used. It is a basic right, although not specified in the Constitution, designed to protect the personal freedom of decision from the risk caused by the enlargement of state functions and info-communication technology.

24 Several rights are derived from this right to control personal information:

4 For a detailed presentation, see Graham Greenleaf, *Data privacy laws in Asia – Trade and Human Rights Perspective* (Oxford University Press, 2014) at p 127ff.

5 Case 17-1 KCCR 668, 99Hun-Ma513 and 2004Hun-Ma190 (26 May 2005) (“Resident Registration Act Case” or “*Collecting and Computerizing Fingerprints and Using Them for Investigation Purposes Case*”).

- (a) the right to prevent the collection and usage of personal information in the absence of the data subject's prior consent;
- (b) the right to access and request correction of collected personal information;
- (c) the right to request suspension of the collection and usage of personal information; and
- (d) the right to request destruction of stored personal information, *etc.*

25 Since then, other landmark judicial or constitutional decisions have confirmed the right to data privacy and specified key concepts under data protection laws in the jurisdiction. In fact, as a commentator explained, “the burden of construing PIPA so as to realise the robust protective vision of lawmakers has fallen to the courts in several key areas”.⁶

26 In a decision of 2015, the Supreme Court in this case has set the standard for determining if a “data handler” should be held contractually or legally liable for failing to take necessary safeguards to ensure the security of data in case of a leak due to hacking.⁷ The facts of the case, in 2008, related to a massive data leak which affected approximately 20 million users of Auction Co, a company owned by eBay Korea, then the largest open market operator in the country. More than 140,000 users initiated a lawsuit against Auction Co to recover damages. The court considered that the company was not responsible for the breach given its security policy, the effectiveness of antivirus technology at the time, and the hacking techniques employed by the infiltrators, and rejected the plaintiffs’ claim.

6 John Leitner, “Data Privacy in South Korea: Can Legislation Transform Protection of Personal Information?”, *Digital Asia Hub* (21 October 2016).

7 According to the Supreme Court, this decision will depend on a number of criteria, among which the universal standard of known security technologies at the time of the incident; the line and size of business of the information and communications service provider (“ICSP”); the overall security measures taken by the ICSP; the cost and benefit accompanied by such security measures; the level of hacking technologies; the development stage of security technology to prevent incidents; the contents of the personal information collected by the ICSP and the scope of damages caused by the data leakage to users. See related article “eBay Korea Not Responsible for Massive Data Leak in 2008: Court” *The Korea Times* (12 February 2015).

27 Additionally, in the *LG Telecom* decision, the Supreme Court defined the responsibilities of an information and communications service provider (“ICSP”) in case of leakage of personal information protected by the Network Act. The notion of “data leakage” is defined as a situation where the ICSP loses the control of personal information to the effect that a third party gets to know its contents. The Supreme Court considered that this qualification did not apply in this case.⁸

28 In the *GS Caltex* decision of 26 December 2012, the Supreme Court established standards by which to assess the liability of data handlers for distress suffered by data subjects through leakage of their personal information. The case involved an employee of an external service provider with access to the customer information of GS Caltex, one of the largest oil refiners in Korea. This employee obtained personal information illegally and intentionally leaked it to the media in order to induce a collective civil lawsuit against GS Caltex. The Supreme Court concluded that the leakage of the plaintiffs’ personal information did not cause an emotional distress that warranted an award of compensation. As a rationale for its decision, it stated that the leaked personal information was only provided to, and copied by a limited number of persons, no third parties appeared to have accessed the information as all relevant storage devices had been retrieved or destroyed, and no additional damage such identity theft, illegal use of another person’s name, or any additional leakage of personal information was caused to the plaintiffs.⁹

29 On 7 April 2017, the Supreme Court handed down a landmark decision in the so-called “*Homeplus Case*”. This decision establishes the requirements to obtain consent from data subjects and provides a standard to distinguish whether a transfer of personal information should be qualified as “provision” or “outsourcing” of personal data under the PIPA – a qualification that has important consequences, at least in theory, as the “provision” of personal data is subject to the data subject’s consent, with criminal liability attached.

8 Supreme Court Decision 2011Da24555, 2011Da24562 (16 May 2014).

9 Supreme Court Decision 2011Da59834, 59858, 59841 (26 December 2012).

30 Homeplus, a major retailer operating a chain of discount stores in Korea, had concluded business partnership contracts with insurance companies whereby it sold them the data of 24 million customers which it had obtained through promotional giveaway events. The case outraged Korean citizens and Homeplus was sued in court for violation of the PIPA. The case hinged on the decision whether (a) Homeplus had collected the personal information through fraud or other unlawful means; and (b) whether the transfer of the personal information to the insurance companies constituted a “provision” or “outsourcing” under Korean law.

31 On the first point, the Supreme Court stated that “the data handler’s act of obtaining the consent at question should not be viewed in isolation but the entire process for obtaining such consent should be examined”. The court found that in this assessment, reference must be made to “socially accepted norms”, based on the motives and purposes for collecting the personal information, the relevance between the purpose for collection and the personal information that is to be collected, specific methods used for collection, compliance with the PIPA and other relevant laws and regulations, the contents and volume of the obtained personal information, and whether any sensitive information or particular identification information was also collected. On that basis, the Supreme Court found that Homeplus had “acquired personal information or obtained consent to the processing of personal information by fraud or other unlawful means”. It found that Homeplus had misled customers into believing they were participating in a promotional giveaway event, while they had collected personal information that was unrelated to the event with the intention to provide the data to third parties. While customers had received written disclosure that their information could be sold to insurance companies, the court ruled that they could not clearly understand the consequences of giving their consent: the font size of the text on the coupon was one millimetre, so that it was impossible to consider that separate notice had been given for each type of consent. The volume of personal information collected by Homeplus and the profits it earned by selling the personal information to third parties were also factors considered by the court.

32 On the second point, the Supreme Court stated that different factors should be taken into account, such as the purpose and method of

obtaining the personal information, whether consideration had been received in exchange for the personal information, whether the recipient was actually being supervised and managed, the impact on the need to protect the personal information of data subjects or users, and which parties actually needed to have access and use the personal information. While the six Homeplus executives who were prosecuted for violations of the PIPA were acquitted, the Korean Fair Trade Commission issued a heavy fine against Homeplus, and customers filed suits seeking civil remedies.

ii *Impact of supra-national data protection frameworks*

33 Korea has ratified the International Covenant on Civil and Political Rights (“ICCPR”) and the Optional Protocol to the International Covenant on Civil and Political Rights in 1990. It has not yet signed nor ratified the second Optional Protocol to the International Covenant on Civil and Political Rights.

34 Beyond these general commitments effectively reflected in the PIPA, Network Act and other relevant data protection texts in Korean law, regional data protection frameworks are driving important changes in the Korean legal system.

35 In October 2010, the Korean government joined as an observer on the Consultative Committee of Council of Europe Convention 108.

36 Korea is an Asia-Pacific Economic Cooperation (“APEC”) Member economy. KCC (as of May 2011) and MOIS (as of 2014) have joined the Cross-border Privacy Enforcement Arrangement, and Korea joined the APEC CBPR system in June 2017, following the US, Mexico, Canada and Japan. It is expected that KISA will apply to the Joint Observatory Body (“JOB”) as an Accountability Agency in Korea under the CBPR scheme in the second half of 2018.

37 In 2015, Korea initiated the formal process for the EU to recognise that Korea offers an adequate level of protection in application of Article 25(6) of Directive 95/46/EC. On 10 January 2017, the European Commission announced that it will actively engage with key trading partners in East and South-East Asia, starting with Japan and Korea in

2017.¹⁰ It is known that Korea and the EU have been discussing the objective of a “partial” adequacy finding, according to which the decision would apply to the sector covered by the Network Act and administered by KCC – in practice, the online-related activities of almost all major businesses. In November 2017, European Commissioner Věra Jourová met with Mr Lee Hyo-seong, Chairman of KCC and Mr Jeong Hyun-cheol, Vice President of KISA, to exchange views on ways to further strengthen co-operation between the EU and Korea on data protection and data flow issues.¹¹

38 To a certain extent, it is envisaged that the extraterritorial effects of the European General Data Protection Regulation will have a significant impact on the data processing activities of businesses in Korea, especially on Korean companies in the EU and their Korean parent companies.

C STATUTORY RULES ON INTERNATIONAL DATA TRANSFERS

39 As mentioned above, the PIPA is the general comprehensive data protection Act in Korea. On top of the PIPA, specific laws apply to data protection in some sectors, such as the Network Act on the protection of personal information related to information and communications services, the Credit Information Act, on the protection of data related to credit information, and the Location Information Act. Each of those statutes has been specified in secondary legislation and administrative regulations.¹²

10 See <<http://europa.eu/rapid/attachment/MEMO-17-15/en/international-transfert-data-08%20final%20.pdf>> (accessed 10 April 2018).

11 See European Commission – Statement, “Press Statement by Commissioner Věra Jourová, Mr Lee Hyo-seong, Chairman of the Korea Communications Commission and Mr Jeong Hyun-cheol, Vice President of the Korea Internet & Security Agency” (Press Release Database, 20 November 2017).

12 See the Enforcement Decree of the Personal Information Protection Act, the Enforcement Decree of the Act on Promotion of Information Communication Network Usage and Information Protection and the Enforcement Decree of the Use and Protection of Credit Information Act.

40 The main provisions on cross-border data transfers are contained in the PIPA and the Network Act. Specific regulations apply in other sectors, which will be briefly mentioned.

i *Data transfers under PIPA (Article 17)*

41 Article 17(1) of the PIPA (“Provision of Personal Information”) provides that a “personal information controller” may transfer data to a third party only:

- (a) with the data subject’s consent; or
- (b) if the purpose of the transfer corresponds to the purposes for which the data were originally collected, pursuant to Article 15(1) subparagraphs 2, 3, and 5 of the PIPA.¹³

This rule applies whether the recipient of the data is located inside or outside Korea.

42 Article 17(2) of the PIPA specifies the conditions under which the data subject’s consent must be given to be valid under Article 17(1). The personal information controller must inform the data subject of:

- (a) the identity of the recipient;
- (b) the purpose for which the recipient will use such information;
- (c) particulars of the personal information to be provided;
- (d) the period for which the recipient retains and uses the personal information; and

13 The purposes listed in Art 15(1) subparas 2 3, and 5 are as follows:

2. Where the communication of data is required to comply with a legal obligation.

3. Where it is required for a public institution to perform its national statutory mission.

5. Where it is deemed necessary to protect from an impending danger the life, bodily integrity, or economic interests of a data subject or of a third party, when the data subject or his/her legal representative is not in a position to express intention, or prior consent cannot be obtained as the individual’s contact details are unknown.

- (e) the fact that the data subject is free not to give his consent, and any negative consequence for the data subject resulting from his denial to consent.

The data subject must be informed if change occurs in any of the above.

43 Article 17(3) applies in cases where data are transferred to a third party overseas. A personal information controller shall then inform the data subject of the elements listed in Article 17(2), and separately obtain the data subject's consent to the transfer of his personal information to the foreign party.

44 Article 22 specifies the method for obtaining consent under all consent-related provisions in the PIPA. It explicitly provides that the data controller must present requests for consent to the data subject "in an explicitly recognizable manner which distinguishes matters requiring consent from the other matters, and obtain his/her consent thereto, respectively". This Article further mentions that the data subject's consent must be obtained separately for the original collection and use of personal information (Article 15(1) subparagraph 1), for the provision of personal information to third parties (Article 17(1) subparagraph 1), for the processing of sensitive information (Article 23(1) subparagraph 1), and for the processing of national identifiers (Article 24(1) subparagraph 1).

45 Article 17(3) further specifies that the personal information controller shall not enter into a contract for the cross-border transfer of personal information in violation of the Act.

ii Data transfers under Network Act (Article 63)

46 Article 63 ("Protection of Personal Information Transferred Abroad") of the Network Act was roughly similar to Article 17 of the PIPA until it got a massive overhaul in 2016, with effect from 30 September 2016.

a Principle: Consent required

47 As a rule, the ICSP and the recipient of personal information from an ICSP (together referred to as “Extended ICSPs”) must obtain the user’s consent to transfer data overseas (Article 63(2) of the Network Act). This obligation arises from the rules of the Network Act which apply to “Extended ICSPs”, and not “ICSPs” alone. The user’s consent must be obtained after providing him with the following information (Article 63(3)):

- (a) the items of personal information transferred;
- (b) the country to which the personal information is to be transferred, date and time, and methods of transfer;
- (c) the name of the person to whom the personal information is to be transferred (*ie*, the name of legal entity and contact person); and
- (d) the purposes of use of the data by the recipient, and the period for which the data will be retained and used.

48 When Extended ICSPs transfer personal information overseas based on the user’s consent, Article 63(4) of the Network Act further prescribes that they take “protective measures” which must be agreed and formalised in a contract between the exporter and importer. These measures are defined by Presidential Decree as technical and administrative measures for protecting personal information, measures for dealing with complaints and resolving disputes in cases of data protection infringement, and any other measures necessary for protecting the users’ personal information.¹⁴

49 As a rule, the consent requirement applies to:

- (a) the provision of personal data to a third party, when the transfer is for the third party’s benefit (including cases where the personal information of Koreans is accessed from abroad);

14 See Art 67(2) of Personal Information Protection Act’s Presidential Enforcement Decree.

- (b) the outsourcing of processing of personal information to a processor; and
- (c) the storage of personal data outside of Korea.

b Exceptions to user's consent requirement

50 Extended ICSPs may outsource or store personal information overseas without the user's consent in specific circumstances detailed in Article 63(2) of the Network Act. These circumstances are when:

- (a) an agreement for the provision of information and communication services has been entered into by the Extended ICSP and the user;
- (b) the cross-border transfer of the personal information is necessary to increase user convenience; and
- (c) the Extended ICSP has disclosed to users all the items of information referred to in Article 63(3) via its privacy policy, or individually notified them via a method prescribed by statute, such as e-mail.

c Proposed reforms

51 A Bill to amend the data transfer provisions of the Network Act is currently pending in the National Assembly of Korea, reportedly "following the ongoing negotiations with the EU Commission, domestic developments, and Korea's steps to join APEC CBPRs (as yet incomplete)".¹⁵ If passed in their current version (which is uncertain), these amendments would bind the overseas recipient by similar requirements as apply to the transferor, and KCC will have authority to suspend cross-border data transfers if the users' rights are severely violated.

52 Two more exceptions to the consent requirements would be added:¹⁶

15 Graham Greenleaf, "Questioning 'Adequacy' (Pt II) – South Korea" (2018) 151 *Privacy Laws & Business International Report*.

16 Graham Greenleaf, "Questioning 'Adequacy' (Pt II) – South Korea" (2018) 151 *Privacy Laws & Business International Report* at p 4.

- (a) if Korea is a party to “other international agreements” which include “specific provisions concerning cross-border transfer of personal information”; and
- (b) where the overseas recipient of the transfer has been certified under the Personal Information Management System (“PIMS”) certification scheme (see “Certification, trustmarks and privacy seals”, below) or other certification designated by KCC.

53 The exact consequences of the proposed amendments are still unclear, hence, they will require careful monitoring as they will have a significant impact on the cross-border data transfer provisions of Article 63.

iii Role of regulatory authorities under data transfer provisions in PIPA and Network Act

54 Neither the PIPA nor the Network Act specifically authorise or prescribe specific roles for the different competent authorities to implement these cross-border transfers of personal data under the Acts. For instance, there is no need to provide prior notice to, or obtain prior authorisation from these authorities for the cross-border transfer of personal data under Korean data protection laws.

55 MOIS has published a guide to the interpretation of the PIPA which provides commentary on how to interpret all the provisions of the PIPA, including those relating to the cross-border transfer of personal information, available in Korean.¹⁷

56 In 2012, KCC also published a guide on the interpretation of Korean data protection laws for ICSPs that contains information relating to the cross-border transfer of personal information.¹⁸ However, these guides are not particularly noteworthy or useful as they only contain fairly basic and general explanations.

17 Available at <<http://bit.ly/2CNMuqY>> (in Korean only) (accessed 10 April 2018).

18 Available at <https://www.kisa.or.kr/public/laws/laws3_View.jsp?mode=view&p_No=259&cb_No=259&d_No=7&ST=T&SV=#> (in Korean only) (accessed 10 April 2018).

57 As mentioned above, however, if the amendments to Article 63 of the Network Act are passed in their current version, KCC will have the power to suspend cross-border data transfers if the users' rights are severely violated.

iv *Restriction on international data transfers in specific sectors*

58 In addition to the PIPA and the Network Act, other restrictions apply to cross-border data transfer in specific sectors, in particular in finance and health. These will be dealt with below (see "Data localisation", below).

D DEFAULT POSITION, SCOPE AND TERRITORIAL EFFECT OF DATA TRANSFER PROVISIONS

i *Default position*

59 The basic approach of Korean data protection laws is that cross-border transfers of personal information should be permitted in principle, subject to certain exceptions.

60 The default rule is different in specific sectors, which require the storage of information in Korea, and forbid the transfer of the personal information covered by these laws as a matter of principle (see "Data localisation", below).

ii *Territorial scope*

61 Neither the PIPA nor the Network Act expressly specifies the territorial scope of its application. MOIS has yet to announce its position regarding the applicability of the PIPA to foreign data controllers. However, KCC has long held that the Network Act will be applicable to any ICSPs located in a foreign jurisdiction that conduct business involving Korean residents or citizens.

62 Case law from the lower courts supports this position. Thus, in November 2015, the Seoul Central District Court ordered Google Inc to comply with Korean data protection law on the basis that it provided its

services based on the location information of South Korean residents, even if it is not located in Korea.¹⁹ In this case, directly triggered by the Snowden revelations and the so-called *Schrems* case in Europe, the court reportedly ordered Google Inc (not Google Korea) to release certain details of records of personal information it has shared with third parties (*ie*, foreign public authorities).²⁰

63 The Seoul High Court which reviewed the case on appeal handed down a slightly different decision on 16 February 2017. It ordered Google Inc to disclose “*certain*” details of records of personal information it has shared with its third parties, and ordered Google Korea to disclose “*any*” details of records of personal information it has shared with third parties. Both parties appealed the decision, and the case is currently pending in the Korean Supreme Court.

iii *Organisations covered by data transfer provisions*

64 The PIPA, being a baseline legislation, regulates personal information held by all Korean controllers under the meaning of the Act. As noted above, the Network Act more specifically regulates personal information processed by ICSPs, *eg*, online game service providers, Internet portals, social networking service (“SNS”) providers and e-commerce service providers, *etc*. The Network Act defines “information and communications service providers” as telecommunications operators and other providers of information or intermediate information services who make commercial use of the services rendered by telecommunications operators.²¹

65 In practice, the Network Act covers most online activities, whereas the PIPA would refer mostly to offline activities.

19 Park Whon-il, “Government Access to Personal Data” <http://www.koreanlii.or.kr/w/index.php/Government_access_to_personal_data> (accessed 10 April 2018).

20 Diana Tomale, “Seoul Court Orders Google Inc to Disclose List of Personal Information of South Korean Users Reportedly Shared with Third Parties” *Korea Portal* (10 November 2015).

21 Act on Promotion of Information Communication Network Usage and Information Protection Art 2(3).

66 Within this scope, Korean law distinguishes between transfers of personal information to “controllers” and “processors”. In the case of cross-border transfers from a controller in Korea to an overseas controller, the PIPA requires the consent of data subjects, but not in cases where transfers are made from a controller in Korea to an overseas processor. In contrast, the Network Act, in principle, requires the consent of data subjects in both cases.

67 Korean data protection laws do not exempt categories of sectors or companies (*eg*, small and medium-sized enterprises (“SMEs”)) from the application of provisions in the Act, including the provisions relating to cross-border data flows.

iv Data covered by data transfer provisions

a Definition of “personal information”

68 The regulation of cross-border transfers of personal information applies to *all personal information* respectively covered by the PIPA and the Network Act.

69 Article 2 of the PIPA defines personal information as “information relating to a living individual that makes it possible to identify the individual by his/her full name, resident registration number, image, etc (including information which, if not by itself, makes it possible to identify any specific individual if combined with other information)”.

70 Article 6 of the Network Act retains a similar definition:

Personal information means the information pertaining to any living person, including the code, letter, voice, sound and image, etc, that make it possible to identify such individual by his/her name and resident registration number, etc (including the information that does not, on its own, permit direct identification of a specific individual, but that does identify specific individual when it is easily combined with other information).

71 The definition of personal information has been discussed in the Korean courts. For instance, in the “*Smartphone IMEI Serial Number Case*” the Seoul Central District Court judged that the IMEI and USIM serial numbers of smartphone numbers could be “easily combined” with

other identifiable information (*ie*, subscribers' data) and lead to the user's identity, and hence are personal information under the law.²²

72 In its decision of 20 February 2017 in the Google case reported above, the Seoul High Court considered whether non-identifiable information, stripped of names and resident registration numbers, amounted to personal information. While Google argued that such non-identifiable information was not subject to the disclosure rule, the High Court ruled that even non-identifiable information must be treated as personal information if the individuals could be identified by combining the non-identifiable information with other information. As mentioned above, the case is currently pending in the Supreme Court of Korea.

b “De-identification guidelines”

73 The concepts of anonymisation, pseudonymisation and de-identification of personal information are not firmly acknowledged by data privacy experts in Korea yet, but it is generally understood that data that have been anonymised are not deemed as personal information because they can no longer be used to identify a specific individual. Therefore, data that have been anonymised will no longer be subject to the PIPA, Network Act or other relevant laws. However, pseudonymised data or even encrypted data which could be later re-identified are still deemed as personal information, thus subject to Korean data protection laws.

74 In this regard, it is worth noting that on 30 June 2016, the Korean authorities responsible for enforcing data protection and privacy laws and regulations have jointly issued guidelines stating their official position on the de-identification of personal information. The Guidelines on Personal Information De-identification Measures (“De-Identification Guidelines”) has been jointly adopted by MOIS, KCC, the Financial Services Commission, the Ministry of Science and ICT, the Ministry of Health and Welfare and the Office for Government Policy Coordination, with the objective to support the big data industry and

22 Seoul Central District Court Decision 2010GoDan5343 (23 February 2011).

related companies.²³ While not legally binding, the De-Identification Guidelines is significant given the number and quality of its signatories.

75 The De-Identification Guidelines provides an indication of the extent to which controllers may use pseudonymised or encrypted personal information.²⁴ It namely specifies:

- (a) the criteria, procedures and methods for the de-identification measures necessary for utilising big data; and
- (b) the criteria for determining what qualifies as personal information.²⁵

76 The De-Identification Guidelines also specifies that while information which is presumed “de-identified” in accordance with the guidelines may be used and provided to third parties without obtaining the data subject’s further consent, the data handler must still implement certain safeguards in order to prevent re-identification.

77 By adopting these guidelines, the above-mentioned authorities have sought to reduce much of the existing ambiguity associated with the concepts of “personal information” and “de-identification”, and to lay the foundation for utilising big data while promoting the security of personal information in Korea.

c Sensitive personal information

78 Special provisions apply to sensitive personal information, defined by Article 23 of the PIPA as personal information “including ideology,

23 Kwang-Bae Park & Hwan-Kyoung Ko, “Highlights of the ‘Big Data Guidelines for Data Protection’” *Lee&Ko Newsletter* (January 2015). See also Graham Greenleaf, “2014–2017 Update to Asian Data Privacy Laws – Trade and Human Rights Perspectives” (12 July 2017) UNSW Law Research Paper No 47, 2017, at pp 13–14.

24 “‘Guidelines on De-identification Measures’ and the ‘Comprehensive Guide to Data Protection Laws and Regulations’ Newly Announced” *Lee&Ko Newsletter* (July 2016).

25 See Graham Greenleaf, “2014–2017 Update to Asian Data Privacy Laws – Trade and Human Rights Perspectives” (12 July 2017) UNSW Law Research Paper No 47, 2017, at pp 13–14.

belief, admission to, and exit from trade unions or political parties, political opinions, health, sexual life, and other personal information which is likely doing harm to privacy of data subjects, as prescribed by the Presidential Decree”. Such data may only be processed with the user’s specific consent or when the law allows or requires their processing.

d “Foreign data”

79 There has been no ruling on whether the data protection laws of Korea apply to individuals whose data have been imported into Korea by a local entity or not. But the general understanding is that such “foreign data” are afforded the same protection as “domestic data”, if they are handled by a controller or processor that is subject to Korean data protection laws.

e Data in transit

80 Neither is it clear whether the law applies to “data in transit” or if such data are excluded from the scope of application of the law or specific provisions. However, it seems reasonable to presume that if data only flow through the network of a Korean controller or processor and are neither stored, viewed, edited, deleted or otherwise processed in Korea, Korean data protection laws will not be applicable, or at least that Korean authorities will be reluctant to enforce Korean laws against them.

E DATA LOCALISATION

81 As a rule, Korean data protection laws do not prescribe data localisation requirements. Although the data subject’s consent mentioned above is express opt-in consent, this type of consent requirement is commonly found in all Korean data protection laws, and thus, this requirement does not necessarily imply that Korea data protection laws require companies to establish onshore data storage in the jurisdiction by default.

82 However, data localisation measures apply in the financial sector.

83 Thus, the Regulation on Supervision of Electronic Financial Transactions prohibits the cross-border transfer of identification information held by financial institutions in Korea, and requires that these institutions install their servers and disaster recovery facilities in Korea.

84 Only information processing systems with limited effect on the security and reliability of electronic financial transactions, and which may thus be designated as “non-critical”, may be established abroad.

85 However, the qualification of “non-critical information processing system” may not be attached to any system processing particular identification information (*ie*, resident registration numbers, passport numbers, driver’s licence numbers and alien registration numbers) or personal credit information covered by the Credit Information Act. In effect, therefore, the processing of any particular identification information or personal credit information of individuals in a foreign jurisdiction is effectively prohibited.

86 Furthermore, specific restrictions are applicable to the outsourcing of data processing in the financial sector under the Regulation on Financial Institutions’ Outsourcing of Data Processing Business & IT Facilities, last amended in 2015.²⁶ Financial companies in Korea must report certain matters prescribed by law on the outsourcing of data processing to the Financial Services Commission (“FSS”), regardless of whether such data processing takes place in Korea or a foreign jurisdiction. Depending on the specific nature of the data processing, financial companies may be subject to *ex ante/ex post* reporting obligations.

87 Thus, the combined application of these Regulations imposes the requirement that certain financial companies and electronic financial business operators install their servers and other electronic facilities in Korea, and also prohibits financial business operators from processing

26 See Financial Services Commission, “Revision to Regulation on Financial Institutions’ Outsourcing of Data Processing Business & IT Facilities” (Press Release, 9 June 2015).

any particular identification information or personal credit information of Korean citizens in a foreign jurisdiction.

88 In addition, in the health sector, the Enforcement Rule of the Medical Service Act and the Standards of Facilities and Equipment for Management and Retention of Electronic Medical Records (“EMRs”) provide that the physical location of an EMR system and its backup equipment shall be restricted to Korea, and thus, it is prohibited to transfer EMRs generated at a hospital in Korea to an overseas location. Such restrictions have been implemented to enable immediate response, investigation and restoration following the occurrence of a physical security incident and to minimise the leakage of medical information.

89 In such cases, data are required to be physically stored in Korea and it is prohibited to transfer copies of the relevant data abroad.

90 The territorial scope of data localisation requirements is based on whether the company is located in Korea and whether personal information is collected from individuals in Korea.

91 Both local and foreign companies are subject to the same data localisation obligations, under the law and in practice.

92 There do not appear to be any procedures which grant an exception for the data localisation requirements above.

93 Data localisation requirements are not applicable to anonymised data, as the Regulation on the Outsourcing of Data Processing by Financial Companies clearly states.

94 Encryption is required in order to outsource the processing of particular identification information, but even encrypted particular identification information is prohibited from being transferred abroad.

95 The Regulation does not clearly state any position with respect to the treatment of pseudonymised data.

96 However, in cases where the processing of financial transaction information of individual customers is outsourced to a third party, reporting obligations to FSS are exempted in cases where it is impossible

to identify the data subjects of such financial transactions. Although not absolutely certain, it appears that data localisation requirements may not apply in cases where measures recommended by the De-Identification Guidelines have been implemented. It is this reporter's understanding that the data localisation provisions are already being enforced but there do not appear to be any enforcement cases as of yet related to a violation of such provisions.

F INTERNATIONAL DATA TRANSFERS AND FREE TRADE AGREEMENTS

97 Korea has signed various bilateral or multilateral free trade agreements ("FTA") with other jurisdictions that cover sectoral or general transfers of personal information.

98 Korea signed the Korea-ASEAN FTA in 2009 where, for the first time, the text of the agreement included clauses on personal information protection. For instance, Article 13 of the Agreement on Trade in Services provides that:

Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between Parties where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Party of measures necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: ... (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.

99 ASEAN and Korea have also agreed to increase co-operation in information and communications technology ("ICT"), which may include "exchanging information and expertise on ICT policies, creation of ICT-related services, provision of e-government services, content development, network security and protection of privacy" (Article 8 of the Annex to the ASEAN-Korea Framework Agreement on Comprehensive Economic Cooperation).

100 The Korea-EU FTA contains similar clauses in its chapters on e-commerce and trade in services. The Korea-China FTA also includes clauses regarding the transfer of data in e-Commerce.

101 Article 15.8 of the Korea-US FTA (“Cross-border information flows”) in the Chapter on e-commerce only provides that: “Recognizing the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, the Parties shall endeavour to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders.”

102 Korea also participated in negotiations for the TiSA (Trade in Services Agreement) which includes clauses regarding the transfer of data.

103 In Korea, international treaties are afforded the same status as an Act in the legal hierarchy. However, following the ratification of the Korea-US FTA and the Korea-EU FTA, the Korean government promulgated a new regulation entitled the “Regulation on the Outsourcing of Data Processing and Computing Facilities and Equipment by Financial Companies” (later retitled “Regulation on the Outsourcing of Data Processing by Financial Companies” on 22 July 2015) prescribing certain cross-border data transfer provisions in the financial sector.

G DATA TRANSFER MECHANISMS

i Preliminary issues

104 Korea’s largest percentage of trade and investment is conducted with other Asian countries. The cross-border transfer of personal information is inherent to trading with, and investing in other Asian countries. From the perspective of multinational business operators, therefore, the existence of multiple cross-border transfer systems in Asia presents significant challenges.

105 If various legitimising grounds such as consent, adequacy findings or “white lists”, Binding Corporate Rules (“BCRs”), Standard Contractual Clauses (“SCCs”), *etc.*, are required for each jurisdiction, the

specific requirements and the interpretation of each of these grounds are likely to be also different for each jurisdiction. Further, such difficulties will become exacerbated with the increased usage of cloud computing.

106 In Korea, the most frequently used data transfer mechanism is prior, explicit, opt-in consent by data subjects. From a legal standpoint, a crucial factor that influences the decision of companies in choosing a particular data transfer instrument is the obtainability of consent from data subjects. Indeed, business operators may easily obtain consent from data subjects (in many cases, employees) or may find it difficult to obtain such consent without incurring significant costs.

107 As explained below, the types of situations where the data subjects' consent is required for cross-border data transfers can be complex.

a When a data exporter is subject to PIPA

108 A typical case could be when an offline business operator processes personal information in its possession or when an online company processes employee-related data such as human resources data. The consent of data subjects will not be required when cross-border data transfers can be characterised as the outsourcing of data processing. This is because the PIPA provisions relating to cross-border data transfers cover transfers of personal information between controllers. However, in cases where data processing is outsourced (*ie*, transfers between a controller to a processor), the same rules apply to both domestic transfers and cross-border transfers of personal data. In other words, the consent of data subjects is not required but such outsourcing must be conducted pursuant to a written instrument (mainly contracts) between the controller and the processor, the details of such outsourcing must be disclosed (on the controller's Internet homepage, *etc*) and certain other restrictions may also apply.

b When data exporter is subject to Network Act

109 Under the Network Act, consent requirements differ from those under the PIPA because the Network Act governs the personal information of ICSPs and users that receive information and communications services. From the perspective of the PIPA, ICSPs are

“controllers”, and users are “data subjects”. Specifically, under the Network Act, ICSPs are defined as telecommunications business operators that have obtained a licence, completed registration, or completed reporting (including cases where reporting obligations have been exempted) pursuant to the Telecommunications Business Act and other persons who provide information or intermediate information services commercially by utilising the services provided by a telecommunications business operator. When an ICSP provides the personal information of users to a third party after obtaining consent from users, the third-party recipient may, to a certain extent, also become subject to the Network Act. The consent of users is required in cases where ICSPs and third-party recipients of users’ personal information (as defined earlier as “Extended ICSPs”) provide (including cases where specific personal information is searched only), outsource the processing, or store the personal information of users abroad. However, the Extended ICSPs are permitted to transfer the personal information of users abroad without obtaining user consent if (a) such personal information is transferred for the purposes of outsourcing its processing or storage by a third party; (b) such outsourcing/storage is necessary for performing the information communication services and enhances the convenience of the user; and (c) the Extended ICSP has disclosed all required matters via its privacy policy or individually notified users via a statutorily-prescribed method such as e-mail.

110 Meanwhile, although there has been some demand for transfer instruments that are compatible or that promote global interoperability among business operators in Korea conducting multinational business operations, it is difficult to say that such demand has generally spread throughout the companies in Korea. However, with the increase of countries that have enacted data localisation laws or implemented legal restrictions to cross-border data transfers, the interest in interoperability has grown accordingly.

ii *Liability issues*

111 Korean data protection laws impose, in certain cases, an obligation on the exporter to ensure that the recipient is bound by legally enforceable obligations regarding the protection of the transferred data.

a Liability issues in case of transfers to overseas processor

112 As a rule, Korean data exporters remain liable under Korean law where there has been a breach of the data protection obligations by the data importer overseas. Both the PIPA and Network Act provide that if an exporter (controller) transfers personal information to an outsourced processor, this processor will be treated as an employee of the exporter when their respective liabilities are assessed, in cases where the processor has breached applicable laws when performing the outsourced tasks. As such, the exporter may be held liable to data subjects where it fails to establish that it sufficiently managed and supervised the outsourced processor.

113 In practice, the data exporter is obliged to ensure that the processor complies with all applicable laws and regulations, through pro-active management and supervision of the outsourced processor. This supervision aims to prevent that personal information from being lost, stolen, leaked, inappropriately used or destroyed during outsourcing.

b Liability issues in case of transfers to overseas controller

114 Liability issues will be assessed differently when data transfers are made between controllers, whether under the PIPA or Network Act.

115 From a theoretical standpoint, the exporter could be held liable for damages to data subjects for failing to transfer data without adequate disclosure to data subjects, even if it was aware that the outsourced controller (recipient) had breached, or intended to breach the law in such a way as to cause serious damages to the data subjects. However, there do not appear to be any actual cases where this situation occurred and was challenged in the courts.

iii Role of self-regulation

116 Under the PIPA, PIPC and MOIS are both obligated to promote self-regulation. However, the general approach to self-regulation and self-certification in practice does not appear to be consistent with the approach prescribed by Korean law. Self-regulation is not being actively

conducted in practice, although various laws promote self-regulation, in the area of data protection laws and beyond.

117 A personal information self-regulation programme has been established by MOIS in 2016 in order to promote self-regulation in the area of data protection in Korea.

118 Thus, any organisation that has been designated as a data protection self-regulation organisation is required to establish its own set of regulations and conduct various data protection activities for its member companies. Although this programme is still in the early stages of implementation, MOIS appears to be advocating self-regulation by designating additional data protection self-regulation organisations and by displaying its commitment to promulgating relevant regulations in support thereof.

119 Although a self-certification programme exists for certifying adequate compliance with applicable safety standards for motor vehicle models when manufacturing, assembling and importing motor vehicles, there is no such self-certification programme for personal information. Instead, privacy enforcement authorities (“PEAs”) such as KISA are responsible for overseeing personal information and data protection certification procedures such as “PIMS” or the Information Security Management System (“ISMS”) (see below).

iv “Adequacy findings” and white lists

120 At the time of writing, Korean data protection laws have not recognised the concept of allowing data transfers to jurisdictions that have laws establishing “adequate or comparable data protection standards” (or similar wording) without the consent of data subjects. However, there is a possibility that amendments to relevant data protection law(s) will authorise such data transfers in the future, especially considering that Korea is expected to be recognised by the EU as a country providing adequate levels of data protection.

v *Consent as exception to existence of privacy safeguards overseas*

121 Irrespective of the obligation to obtain the individual's consent for the transfer to be legal, Korean data protection laws do not allow consent to be used to waive the requirement to implement privacy safeguards in the country of destination.

122 Korean data protection laws do not mention the possibility of such a waiver. On the contrary, in the case of a data transfer between a controller and a processor, whether domestic or cross-border, the controller must stipulate in the relevant contract that the processor shall take technical and organisational measures for the protection of personal information. In the case of a cross-border data transfer that is subject to the Network Act, such measures are required to be taken by the foreign recipient (*ie*, controller or processor).

vi *Other one-off exceptions*

123 In the case of a cross-border transfer between a controller in Korea and a processor located overseas and such transfer being subject to the Network Act, the requirement for consent from the user may be exempted if all of the following requirements are satisfied:

- (a) the transfer is necessary for the performance of the contract with the user;
- (b) the transfer is for the enhancement of convenience and benefit to the user; and
- (c) the following information is disclosed in the privacy policy or notified to the users:
 - (i) items of personal data to be transferred;
 - (ii) name of the recipient country, time and method of transfer;
 - (iii) name of the recipient (in the case of a legal entity, its name and contact detail of the data protection officer); and
 - (iv) purpose of use by the recipient and retention period.

124 As said above, KCC has published a guide on the obligations of ICSPs under the Network Act. This guide explains the obligations of ICSPs under the Network Act, including obligations relating to the

cross-border transfer of personal information. However, the guide is not particularly noteworthy or useful as it only contains basic and general explanations.

vii Contracts

125 Although the PIPA and Network Act do not specifically require the data exporter to enter into a contract, the PIPA prohibits concluding with the importer a contract which is not compliant with relevant laws and the Network Act requires certain items to be included in a contract for the transfer of personal information. Based on such provisions in the PIPA and Network Act, it is generally interpreted that a data exporter shall conclude a contract with the importer irrespective of the status of the recipient. Also, other guarantees such as certification (CBPR, BCR, *etc*) are not required for the recipient, and whether other guarantees have been put in place is irrelevant.

126 Korean data protection laws require minimum safeguards or obligations to be incorporated in a contract between a controller (exporter) and a processor (importer).

127 When a controller exports data to a processor overseas, the PIPA requires the contract to stipulate the technical and organisational measures to be taken by the data processor, as in the case of a domestic transfer of data from a controller to a processor. However, the PIPA does not require such contractual stipulations in the case of cross-border data transfers from a domestic controller to a foreign controller. On the other hand, the Network Act requires an agreement as to technical and organisational measures with the data recipient (regardless of whether the recipient is a controller or a processor) and to incorporate this agreement in the relevant contract with the data recipient.

128 Korean data protection laws do not specifically require such third-party beneficiary clauses to be added in the contract between the data exporter and importer. The Civil Code acknowledges the concept of such third-party beneficiary clauses, thus, the data subject as a beneficiary could exercise his rights under the contract if it provides such a third-party beneficiary clause.

129 SCCs have been published by MOIS for contracts between controllers and processors. However, because SCCs do not have binding legal effect, parties are permitted to vary their terms by agreement. In this reporter's experience, SCCs are not effectively utilised in agreements between large corporations in Korea, nor in the case of cross-border transfer agreements.

130 It may be advisable to develop SCCs, to a limited extent, for cross-border transfer agreements between Asian countries. SCCs may provide standard levels of data protection that could overcome differences in applicable laws, local interests in data protection and privacy, and culture. Especially it may be recommendable for SMEs to rely on SCCs because they are likely to lack the capacity to draft and revise separate data transfer agreements.

131 In some cases, data transfer agreements between EU companies and their Korean affiliates are based on SCCs provided under European law. Generally, certain provisions need to be revised to ensure compliance with Korean law.

viii CBPRs

132 In June 2017, Korea received acceptance from the Joint Oversight Panel ("JOP"), which administers the APEC CBPR system, to participate in the system.²⁷

133 Due to stringent data protection regulations in Korea, it has not been necessary to amend the Korean data protection laws for participation in the CBPR system, and no specific challenges or legal issues have emerged in the process of implementing the CBPR system.

134 The CBPR Accountability Agent ("AA") has not been designated yet, but it is expected that KISA will eventually play that role (for which it is known to be preparing). Indeed, KISA is already in charge of overseeing several certification programmes, such as PIMS (compliance

27 APEC Electronic Commerce Steering Group, "Korea Joins APEC Data Privacy Program" (APEC News Release, 27 June 2017).

mainly for privacy requirements) or ISMS (compliance mainly for security requirements) (see below). KISA is generally recognised as the most suitable institution in Korea to serve as the AA under the CBPR system.

135 As it is still in the early stages, many details still need to be worked out on how to implement the CBPR certification process by KISA. It is expected that the conditions for CPBR certification by KISA will be announced in 2018, and that the actual CBPR certification process by KISA will start from 2019. As yet, no Korean company has publicly expressed an interest in being CBPR-certified.

136 Additionally, it appears that KCC and KISA are currently focusing on the harmonisation of existing certification systems such as PIMS and ISMS with the system under the CBPR. KCC, MOIS, PIPC and KISA have yet to announce any particular position on the EU BCRs.

ix *Certification, trustmarks and privacy seals*

137 Today, certification mechanisms, privacy seals and trustmarks delivered in third countries are not considered as valid means for a data exporter to demonstrate compliance with local cross-border data controls under Korean law. However, a Bill for amending the Network Act is currently under review in the National Assembly, which envisages the waiver of prior consent requirements for cross-border transfer of personal information to overseas recipients designated by KCC as having obtained sufficient certification.

138 Today, the current Network Act and PIPA do not allow or accommodate a mechanism of mutual recognition of trustmarks or privacy seals delivered in another jurisdiction.

139 In Korea, the Network Act and PIPA permit a company to have its privacy management practices certified by an accredited agent, and obtain a mark or seal where there is a positive finding.

a Personal Information Management System²⁸

140 KISA is the certification agency of the PIMS scheme. It is a sub-agency of data protection authorities in Korea that has been established to enhance the information and communications network, encourage the safe use thereof, and promote international co-operation and advancement into the overseas market in relation to broadcasting and communications.

141 This certification is voluntary.

142 PIMS certification is provided in order to certify that a comprehensive management system, including managerial, technical and physical security measures, has been established and is being operated in order to systematically and continuously protect personal information within the information and communications network. Review for certification is conducted in accordance with certification standards established by KCC and certification is granted to companies that have satisfied such standards.

143 KISA may, following deliberation and voting by the certification committee, revoke certification in the following cases:

- (a) having received the certification in a false or otherwise unjustifiable manner;
- (b) the certified company fails to undergo *ex-post facto* review, undergo a renewal review, or remedy a non-conforming aspect as requested by KISA during its certification review;
- (c) falsely indicating or omitting to indicate the type of certification, scope of certification, and period of validity when publicising approval of certification; or
- (d) refusing or obstructing an *ex-post facto* review or renewal review.

144 PIMS certification has already been revoked in a certain number of cases.

28 See <http://www.koreanlii.or.kr/w/index.php/Personal_Information_Management_System> (accessed 10 April 2018).

145 Companies may lodge a complaint with KISA under the scheme, either against the negative results of a certification review or a decision to revoke certification.

146 All data protection seals and marks are made available in a public register.

b Information Security Management System

147 KISA is also the certification agency of the ISMS scheme.

148 Certain business operators under the Network Act are required to obtain certification based on their line of business, amount of sales revenue, and the number of users of information and communications services (Article 47(2)). Specifically, the above provisions state that ISMS certification obligations shall apply to certain facilities-based telecommunications service providers as defined under the Telecommunications Business Act, a business operator of clustered information and communications facilities (*eg*, IDC), a tertiary hospital with annual revenue or tax revenue of at least KRW150b or a higher education institution (*eg*, university) with at least 10,000 students. While certification is compulsory for these organisations, other companies may apply for a seal on a voluntary basis.

149 The purpose of ISMS certification is to certify the conformity of management systems to certification standards established by the Ministry of Science and ICT, including any managerial, technical and physical safeguards implemented by a domestic company or organisation to ensure the security and reliability of their information and communications networks. Certification is granted to companies that have satisfied these standards.

150 The Ministry of Science and ICT may revoke the certification on any of the following grounds:

- (a) the company has received the certification in a false or otherwise unjustifiable manner;
- (b) it has fallen short of the standards for certification; or
- (c) it has refused or obstructed the *ex post facto* management.

151 ISMS certification has been revoked in a number of cases. Here again, a mechanism exists for companies to lodge a complaint with the certification agency.

152 All data protection seals and marks are made available in a public register.

153 Under the PIMS scheme, applicable certification standards will differ depending on the type of organisation that is applying, and SMEs are subject to less stringent certification standards.

x *Other data transfer instruments*

154 Under Korean law, no other accountability instruments or data transfer mechanisms, such as BCRs, codes of conduct and ISO certification, are implemented for the purpose of compliance, as they do not have any legal effect. However, some companies in Korea obtain or maintain ISO certifications voluntarily.

H INTERNATIONAL CO-OPERATION BETWEEN KOREAN AND FOREIGN PRIVACY ENFORCEMENT AUTHORITIES

i *Co-operation with foreign privacy authorities in areas other than enforcement*

155 Korean data protection laws currently include provisions that enable privacy regulators in Korea to develop operational co-operation with the PEAs in other jurisdictions. The PIPA provides that “the government shall establish policy measures necessary to enhance personal information protection standards in the international environment” (Article 14) and the Network Act provides that the Government shall mutually co-operate with other nations or international organisations in carrying out certain affairs, including tasks related to the cross-border transfer of personal information and the protection of personal information (Article 62).

156 Korean authorities participate in mutual information sharing and provide co-operation in investigations between enforcement authorities – leveraging existing international co-operation channels such as the

Cross-border Privacy Enforcement Arrangement (“CPEA”) and Global Privacy Enforcement Network (“GPEN”) – using policy co-ordination networks with overseas personal data protection authorities.

157 Notably, KISA (Korea) and ISC (China) concluded a memorandum of understanding (“MOU”) in 2016. Based on the MOU, KISA established a Korea-China Internet Cooperation Center to detect and delete the personal information of Korean citizens exposed on websites in China, in co-operation with the ISC.

158 So far, the Korean authorities have not actively punished legal violations related to cross-border data transfers. One of the main reasons for this reluctance is that no applicable penalties have been prescribed for violations of provisions relating to cross-border data transfers in the PIPA. This was also the case for the Network Act until recent amendments became effective as of 23 September 2016.

159 However, in January 2014, KCC imposed a penalty surcharge of KRW212m and issued a corrective order (to destroy any personal information collected illegally) against Google Inc for collecting personal information without consent in connection with the operation of its Street View service. KCC has expressed the view that it will sanction violations of the Network Act regardless of the nationality of the violating organisation.

ii *Enforcement of cross-border transfer restrictions*

160 Under the Network Act, any ICSP that transfers personal information to a controller without obtaining users’ consent may be subject to a penalty surcharge of up to 3% of sales revenue related to the violative activity. In addition, any ICSP that transfers personal information to a processor abroad in order to outsource the processing or storage of such personal information without providing proper notice or disclosure to users may be subject to an administrative fine of up to KRW20m.

161 Also, KCC may issue a corrective order against an ICSP upon discovering that it committed a violation of the Network Act such as a violation related to cross-border data transfers. Any ICSP that fails to

comply with a corrective order issued by KCC may be subject to an administrative fine of up to KRW30m. However, the PIPA has yet to prescribe any penalties for violations of provisions related to cross-border data transfers.

162 Under Korean data protection laws, PEAs are generally authorised to conduct investigations, demand production of documents and conduct on-site inspections. MOIS is responsible for enforcing the PIPA and KCC is responsible for enforcing the Network Act. PEAs typically initiate investigations upon becoming aware of potential violations on their own or receiving reports/complaints of potential violations from third parties. Further, PEAs generally entrust KISA with the actual handling of investigations as it possesses the necessary resources and capability. As such, KISA is practically involved in almost all investigations related to potential violations of data protection laws. After KISA concludes an investigation and presents its findings, ministry level government authorities such as MOIS and KCC will issue sanctions based on such findings. As mentioned previously, recent amendments to the Network Act prescribing administrative fines and penalty surcharges for violation of provisions related to cross-border data transfers became effective as of 23 September 2016. However, it appears that no cases have been reported thus far where such sanctions have actually been imposed.

iii *International enforcement by privacy enforcement authorities*

163 MOIS, KCC, PIPC and KISA have each joined various international or regional networks but there do not appear to have been any cases where such PEAs have jointly conducted enforcement actions.

164 Korean data protection laws currently do not include provisions for any of the following situations:

- (a) transfer of complaints to competent authorities in other jurisdictions;
- (b) authorisation or prohibition of disclosure to competent authorities in other jurisdictions of information obtained in investigations; and
- (c) assisting other competent authorities in cross-border investigations.

Nor have Korean PEAs published an enforcement policy on either data transfers or data localisation requirements yet.

165 Korean authorities participate in several enforcement co-operation networks or arrangements. PIPC, MOSI and KISA participate in the GPEN, and MOIS (since 2011) and KCC (since 2014) participate in the APEC CPEA.

166 As members of the CPEA, - MOIS and KCC are expected to perform an enforcement role under the APEC CBPRs after Korea commences operation of the CBPR certification system, probably in 2019.

167 It appears that no Korean authority has entered into bilateral arrangements with competent authorities in other jurisdictions to co-operate in the enforcement of privacy laws.

168 In the past, Korean authorities have been involved in co-ordinated efforts involving authorities from many jurisdictions – for example, PIPC has actively participated in the Asia Pacific Privacy Authorities (“APPA”) Forum (convenes twice a year) and the ICDPPC (convenes once a year) in order to promote mutual co-operation between PEAs.

169 Korean authorities have conducted joint investigations between themselves in Korea, but there do not appear to be any cases where a Korean authority has conducted a joint investigation with an authority of another jurisdiction. Neither does it appear that Korean authorities have provided any assistance to an investigation being conducted by a PEA in another jurisdiction and have transferred a complaint to a PEA in another jurisdiction or *vice versa*.

170 It appears that Korean PEAs have never conducted an enforcement action jointly with one of its foreign counterparts nor issued common findings against a foreign controller based in multiple jurisdictions.

Jurisdictional Report

KINGDOM OF THAILAND

Reporter: **David Duncan**
Consultant, Tilleke & Gibbins

A INTRODUCTION

1 Thailand lacks a comprehensive data privacy regime, in the form of what would typically be encountered in major jurisdictions overseas. However, many commentators have erroneously asserted that Thai law contains no provisions of relevance to data privacy. Indeed, the Constitution reflects the concept that people's privacy should be respected and that personal data should not be exploited, and there are general provisions of law that could be used in relation to a wrongful disclosure of one's personal data that causes damage (*ie*, a tort) or in the case such would amount to criminal defamation. Beyond those general provisions, data privacy provisions exist in several other areas of law, such as sector-specific regulations or licence conditions, in provisions setting out protections for certain categories of information, or in requirements specific to certain professions.

2 A Personal Data Protection Bill has been pending in various forms for at least 15 years, which would establish a personal data protection regime that would feature many of the characteristics with which Western data privacy practitioners are accustomed. While many have speculated as to why the Bill has not been enacted, the reality is that there are likely numerous reasons, such as legislative prioritisation, a general lack of concern about personal data protection among the population, and concern about possible disruption to business and investment that may be brought about by a burdensome new regulatory regime. However, as noted elsewhere herein, progress is being made, and the most recent version of the Bill strikes a good balance between legitimate privacy concerns and not being overly burdensome to business.

3 Despite the lack of a conventional data privacy framework at present, cross-border data transfers still occur with regularity. In most

cases, these are simply a function of economics and business, as well as the efficiencies brought about by centralised hosting and cloud services. In practical terms, businesses in Thailand do not face significant difficulties in relation to cross-border data transfers.

B GENERAL LEGAL FRAMEWORK OF INTERNATIONAL DATA TRANSFERS

i *Existing data privacy protections in national legislation*

4 As noted, Thailand lacks a comprehensive data privacy regime, but a Bill to provide for one has been pending for more than 15 years. One of the more recent versions is available on the website of the Council of State, and another even more recent version is available on the Thai government's public consultation website.

5 Were it to be enacted as written in this most recent draft, cross-border data transfers would be addressed in its sections 13(5) and 24, translations of which are as follows:

Section 13 The Personal Data Protection Commission has the power as follows

...

- (5) to announce and impose criteria to protect the delivery of personal information sent or transferred abroad

...

Section 24 In the case the person who controls the personal information sends or transfers personal information abroad, such person is required to comply with the criteria on personal information protection as prescribed by the Commission according to Section 13(5), except:

- (1) where the law requires;
- (2) where consent is received from the owner of the personal information;
- (3) to comply with a contract between the owner of the personal information and the controller of the personal information;
- (4) to protect the benefit of the owner of the personal information who cannot give consent at that time;
- (5) to transfer to a person who received a standard certificate mark to protect the information in accordance with Section 32 or Section 34; or
- (6) others as imposed in regulations.

6 In February 2018, a period of public consultation in respect of the Bill concluded. Over the past years, it has been under the consideration of the Ministry of Information Communications Technology (now the Ministry of Digital Economy and Society), the Office of the Official Information Commission, the Council of State and the Cabinet. Virtually all of the drafts have contemplated the creation of a new Personal Data Protection Commission, but there have been differences in the entity that would function as Thailand's personal data protection authority, whether building the Office of Official Information Commission into a full-fledged data protection regulator, assigning such authority to the forthcoming Office of National Cybersecurity Committee or the Electronic Transactions Development Agency, or building an entirely new agency for that purpose. The most recent draft contemplates that the Office of the Personal Data Protection Commission would be a newly established agency (see below).

7 Meanwhile, in the general case, data privacy is addressed in several general provisions of statute. The Constitution (2017) also addresses personal data protection in its section 32, a translation of which is as follows:

Section 32 A person shall enjoy the rights of privacy, dignity, reputation and family.

An act violating or affecting the right of a person under paragraph one, or an exploitation of personal information in any manner whatsoever shall not be permitted, except by virtue of a provision of law enacted only to the extent of necessity of public interest.

8 Moreover, provisions of the Civil and Commercial Code address liability in respect of wrongful acts pertaining to personal data. The following are translations of relevant provisions:

Section 420 A person who, wilfully or negligently, unlawfully injures the life, body, health, liberty, property or any right of another person, is said to commit a wrongful act and is bound to make compensation therefore.

Section 423 A person who, contrary to the truth, asserts or circulates as a fact that which is injurious to the reputation or the credit of another or his earnings or prosperity in any other manner, shall compensate the other for any damage arising therefrom, even if he does not know of its untruth, provided he ought to know it.

A person who makes a communication the untruth of which is unknown to him, does not thereby render himself liable to make compensation, if he or the receiver of the communication has a rightful interest in it.

9 A wrongful disclosure of personal information could also amount to defamation, under the Penal Code:

Section 326 Whoever imputes anything to another person before a third person in a manner likely to impair the reputation of such other person or to expose such other person to hatred or contempt is said to commit defamation, and shall be punished with imprisonment not exceeding one year or fine not exceeding THB 20,000, or both.

Section 327 Whoever imputes anything to a deceased before a third person, and such imputation is likely to impair the reputation of the father, mother, spouse, or child of the deceased or to expose such person to hatred or contempt, is said to commit defamation, and shall be liable to the same punishment as provided in Section 326.

Section 328 If the offence of defamation is committed by means of publication of a document, drawing, painting, cinematograph film, picture, or letters made visible by any means, gramophone record, or another recording instrument, recording picture or letters, or by broadcasting or spreading a picture, or by propagation by any other means, the offender shall be punished with imprisonment not exceeding two years and fine not exceeding THB 200,000.

Section 329 Whoever, in good faith, expresses any opinion or statement:

- (1) by way of self-justification or defence, or for the protection of a legitimate interest;
- (2) in the status of being an official in the exercise of his functions;
- (3) by way of fair comment on any person or thing subjected to public criticism; or
- (4) by way of fair report of the open proceedings of any Court or meeting, shall not be guilty of defamation.

Section 330 In case of defamation, if the person prosecuted for defamation can prove that the imputation made by him is true, he shall not be punished, but he shall not be allowed to so prove if such imputation concerns personal matters, and such proof will not be of benefit to the public.

...

Section 332 In case of defamation in which judgment is given that the accused is guilty, the Court may order:

- (1) to seize and destroy the defamatory matter or part thereof;
- (2) to publish the whole or part of the judgment in one or more newspapers once or several times at the expense of the accused.

Section 333 The offences in this Chapter are compoundable offences. If the injured person in the defamation dies before making a complaint, the father, mother, spouse, or child of the deceased may make a complaint, and it shall be deemed that such person is the injured person.

10 Similar provisions exist in the Computer Crimes Act BE 2550 (as amended). These translate as follows:

Section 16 Any person who brings into a computer system accessible by the public computer data which appears to be a photograph of another person, where such photograph has been created, edited, supplemented, or modified by an electronic means or any other means, in a manner likely to cause that other person to be defamed, insulted, hated, or embarrassed, shall be liable to imprisonment for a term not exceeding three years and to a fine not exceeding THB 200,000.

If the act under paragraph one is committed against a photograph of the deceased and such act is likely to cause the deceased's parent, spouse, or child to be defamed, insulted, hated, or embarrassed, the perpetrator shall be liable to the same penalty as that provided in paragraph one.

If the act under paragraph one or paragraph two subsists in the bringing into a computer system in good faith, which constitutes a fair comment on any person or matter which is ordinarily made by a member of the public, the perpetrator shall not be guilty.

The offences under paragraph one and paragraph two are compoundable offences.

If the injured person for the offence under paragraph one or paragraph two dies before making a complaint, the parent, spouse, or child of the injured person shall be entitled to make a complaint and shall be deemed to be the injured person.

11 Certainly, these provisions are not specific to data transfers. Indeed, they apply far more broadly. Nevertheless, they can be applied in relation to data transfers that are wrongful or that constitute criminal offences.

12 Going beyond the general case, data privacy provisions exist in several other areas of law, such as sector-specific regulations or license conditions, in provisions setting out protections for certain categories of information, or in requirements specific to certain professions, for example:

- (a) Chapter 4 (“Protection for Information Subject”) of the Credit Information Business Act BE 2545 (as amended) (as relevant to credit bureaus);
- (b) Regulations applicable to telecommunications licensees under the Telecommunications Business Act BE 2544 (as amended), section 50 of which provides that the National Broadcasting and Telecommunications Commission is to *establish measures for user protection concerning personal data, right to privacy and freedom to communicate by means of telecommunications*;
- (c) provisions of the National Health Act BE 2550 (as amended) (as relevant to personal health information);
- (d) provisions of the Financial Institutions Business Act BE 2551 (as amended) (as relevant to banks, credit fonciers, and finance companies);
- (e) conditions of licences issued under the Securities and Exchange Act BE 2535 (as amended) (as relevant to securities companies); and
- (f) conditions of notifications made and licences and registrations issued under the Royal Decree on Control and Supervision of Electronic Payment Service Business BE 2551, section 16(1) of which empowers the Electronic Transactions Commission to prescribe rules, procedures and conditions on custody and disclosure of the personal information of the service users (as relevant to electronic payment licensees), being replaced by the Payment Systems Act BE 2560.

13 Given the various other data protection obligations that are already in effect in many important sectors of the economy, the Personal Data Protection Bill contains provisions to address how the Bill (once enacted) would function in co-ordination with pre-existing laws and regulations.

ii *International commitments*

14 Thailand is party to a host of treaties and international agreements. Among these, Thailand has ratified the International Covenant on Civil and Political Rights, but it has not signed either of the two Optional Protocols. Thailand is also involved in a number of free trade agreements (“FTAs”), both bilateral and multilateral, and some of these contain very general provisions on personal data protection. The following is an example from the Thai-Chile FTA:

Article 11.7: Electronic Commerce

1. Recognizing the global nature of electronic commerce, the Parties shall endeavour to:

...

- (j) take appropriate measures and take into account international standards on personal data protection:
 - (i) notwithstanding the differences in existing systems for personal data protection in the territories of the Parties, each Party shall take such measures as it considers appropriate and necessary to protect the personal data of users of electronic commerce; and
 - (ii) in the development of data protection standards, each Party shall, to the extent possible, take into account international standards and the criteria of relevant international organizations ...

15 However, treaties and international agreements are not self-executing under Thai law. Rather, implementing legislation is required.

16 Thailand is a member of the Asia-Pacific Economic Cooperation (“APEC”), but Thailand does not participate in the APEC Cross-border Privacy Enforcement Arrangement, nor has Thailand joined the APEC Cross-Border Privacy Rules system.

17 Thailand is a member of the Association of Southeast Asian Nations (“ASEAN”) Economic Community. The ASEAN Framework on Personal Data Protection is among the reasons that Thailand has been pursuing the Personal Data Protection Bill, though the Bill predates the Framework by several years.

18 Thailand is not an observer on the Consultative Committee of the Council of Europe Convention 108, and it has not been recognised by the European Union as offering an adequate level of protection on application of Article 25(6) of Directive 95/46/EC. While the European General Data Protection Regulation (“GDPR”) does not have the force or effect of law in Thailand, there are a number of European companies with operations in Thailand, which makes the GDPR relevant in Thailand, in some situations.

iii *Role of privacy enforcement authority*

19 At this stage, Thailand lacks a comprehensive privacy enforcement authority (“PEA”). Whilst some sector-specific authorities, such as the Bank of Thailand, the Securities and Exchange Commission, and the National Broadcasting and Telecommunications Commission, have regulatory purview including personal data protection matters within their respective economic sectors, personal data protection is not their primary focus. However, the version of the Personal Data Protection Bill which underwent consultation earlier this year would, if enacted, provide for the creation of a Personal Data Protection Commission, an Office of the Personal Data Protection Commission, and a Committee of the Office of the Personal Data Protection Commission. Collectively, they would have a wide array of powers. Among these, the Commission would have the authority to impose conditions for the protection of personal data sent or transferred overseas (section 13(5)) and to settle relevant breaches (section 75). Regarding international co-operation, the Office of the Personal Data Protection Commission would, among its powers, have the authority to enter into agreements and cooperate with other organisations, in Thailand and abroad, as relate to the exercise of its powers and duties (section 36(9) of the Bill).

C DEFAULT POSITION, SCOPE AND TERRITORIAL EFFECT

20 In the general case, the law neither authorises nor prohibits international data transfers. Hence, the default position is that it is advisable to obtain consent from each data subject. However, where special provisions of law are applicable, such as in the case of credit information or personal health information, or where one is a

telecommunications licensee, it would be required to obtain consent prior to transfer, except where law or regulations specify an exception. As for the Personal Data Protection Bill, the version which underwent consultation earlier this year would require personal data controllers to act in conformity with conditions imposed by the Commission under section 13(5), except where an exemption would be applicable (see above).

21 In the general case, the law does not use the terms “controllers”, “processors” or “intermediaries”, as relevant to personal data. This is because, generally, the applicable provisions of law are not specific to personal data issues. For the same reason, there are no exclusions for data in transit, nor are there any exclusions for anonymised, pseudonymised or encrypted data. In contrast, the Personal Data Protection Bill would clearly define “personal data controller” and “personal data processor”, with corresponding implications in terms of regulatory obligations.

22 In general, the question of whether Thai law or foreign law is applicable in particular circumstances is addressed in the Act on Conflict of Laws BE 2481 and the Criminal Code. As relevant to wrongful acts, the Act on Conflict of Laws provides (as translated):

Section 15 An obligation arising out of a wrongful act is governed by the law of the place where the facts constituting such wrongful act have taken place.

The foregoing provision does not apply to facts which, having taken place in a foreign country, are not wrongful according to Siamese law.

In no case can the injured party claim compensation or remedies other than those allowed by Siamese law.

23 As relevant to criminal defamation, the Criminal Code provides:

Section 5 Whenever any offence is even partially committed within the Kingdom, or the consequence of the commission of which, as intended by the offender, occurs within the Kingdom, or by the nature of the commission of which, the consequence resulting therefrom should occur within the Kingdom, or it could be foreseen that the consequence would occur within the Kingdom, it shall be deemed that such offence is committed within the Kingdom.

In case of preparation or attempt to commit any act provided by the law to be an offence, even though it is done outside the Kingdom, if the

consequence of the doing of such act, when carried through to the stage of accomplishment of the offence, will occur within the Kingdom, it shall be deemed that the preparation or attempt to commit such offence is done within the Kingdom.

Section 6 Whenever any offence is committed within the Kingdom, or is deemed by this Code as being committed within the Kingdom, even though the act of a co-principal, a supporter or an instigator in the offence is done outside the Kingdom, it shall be deemed that the principal, supporter, or instigator has committed the offence within the Kingdom.

24 This would apply also in considering criminal offences specified under other Acts, except where those other Acts provide otherwise.

25 Hence, there are many scenarios in which Thai law could apply to data transfers. In theory, it would even be possible that a person abroad whose data were imported into Thailand could avail himself or herself of provisions of Thai law.

D DATA LOCALISATION

26 In the general case, data localisation is not required in Thailand.

27 However, some sector-specific provisions effectively require the storage of some data in covered businesses in Thailand. Examples include licence conditions applicable to electronic payment licensees and regulations applicable to credit bureaus.

E DATA TRANSFER MECHANISMS

28 Given the lack of a comprehensive data privacy regime in Thailand, the data transfer mechanism most frequently used is obtaining consent from each data subject. In the general case, there is no provision for adequacy findings, white lists, binding corporate rules, certifications, trustmarks, privacy seals, codes of conduct or ISO certification, as relevant to data privacy. The most recent draft of the Personal Data Protection Bill contemplates that it would also be permissible for a personal data controller to transfer personal data to recipients that (a) were certified by the Office of the Personal Data Protection Commission as meeting applicable data protection standards (to be

promulgated in regulations); or (b) have received a certification mark from a foreign agency or international organisation that the Personal Data Protection Commission has determined provides for protection equivalent to the requirements under the Thai Personal Data Protection Act. It also leaves open the possibility that additional transfer mechanisms could be permitted by promulgation of ministerial regulations to that effect.

29 As a general matter, it would be helpful for the law to expressly specify situations in which consent of the data subject would not be required, so as to relieve the burden of capturing consent. The Bill does that, to some extent. However, as a practical matter, there is little demand at present for such alternative mechanisms because (a) capturing consent is not too terribly burdensome; and (b) personal data protection is not an area of major interest among the populace.

30 In the general case, a Thai data exporter is not expressly required to have in place legally enforceable obligations regarding the protection of personal data when transferring data overseas. Nevertheless, it remains possible that a Thai data exporter could be liable in respect of a breach by a data importer outside Thailand. For that reason, a Thai data exporter would have natural motivation to protect itself contractually. Standard contractual clauses for data protection matters have not been produced by any government authorities. We have seen some attempts among clients to impose European standard contractual clauses, but such are generally excessive, relative to the current Thai data protection position. Such clauses generally would impose additional obligations and additional liability on a Thai data exporter, relative to what is applicable to the Thai data exporter by virtue of statute.

31 Where sector specific data protection requirements are applicable, some of these specify permissible reasons for transfer of personal data. Examples include those in regulations issued under the Telecommunications Business Act and in provisions of the Credit Information Business Act. However, no such exceptions exist in the general case.

Jurisdictional Report

SOCIALIST REPUBLIC OF VIETNAM

Reporter: **Waewpen Piemwichai**
Foreign Registered Attorney, Tilleke & Gibbins

A BACKGROUND INFORMATION

1 Currently, Vietnam does not have restrictions on international data flow. In general, business entities as well as individuals in Vietnam are allowed to transfer the personal information of their customers (and other data subjects, such as their employees, vendors and partners) outside of Vietnam, provided that prior consent from the customers/data subjects has been obtained.¹ In certain sensitive transactions, such as transfer of information classified as state secret or sensitive data under banking laws/regulations, in addition to consent from the customers/data subjects, the person transferring such information must also encrypt the information before the information can be transferred.²

2 Due to the significant increase in cyberattacks in Vietnam, which afflict thousands of network information systems and cause a loss of thousands of billions of Vietnam dong each year, the Ministry of Public Security (“MOPS”) has recently drafted a Law on Cybersecurity (“Draft Cybersecurity Law”) in order to stipulate principles and conditions for assuring the security of information and information systems in cyberspace, despite the fact that there are other existing legislation which deal with cyber incidents in Vietnam (such as the Law on Network

1 For example, Civil Code (No 91/2015/QH13) Art 38(2); Law on Information Technology (No 67/2006/QH11) Art 21(1); Law on Network Information Security (No 86/2015/QH13) Art 17(1)(a); Law on E-Transactions (No 51/2005/QH11) Art 46(2); Law on Consumer Protection (No 59/2010/QH12) Art 6(2)(b) and Decree No 52/2013/ND-CP on e-commerce (hereinafter “Decree 52”) Art 70(1); *etc.*

2 See Art 16 of Decree No 33/2002/ND-CP on detailing the implementation of the Ordinance on the protection of state secrets and Arts 21(2) and 35(2) of Circular No 31/2015/TT-NHNN regulating safety and confidentiality of banking information technology systems (hereinafter “Circular 31”).

Information Security³ and Decree No 72/2013/ND-CP on management, provision and use of Internet services and online information (“Decree 72”), both of which are under the authority of the Ministry of Information and Communication).

3 The Draft Cybersecurity Law, among its other provisions, introduces the principle of data localisation⁴ to Vietnam, requiring, in particular, that foreign enterprises (*ie*, companies incorporated outside of Vietnam) when providing telecommunication (“telecom”) and Internet services in Vietnam must locate their representative offices, and any servers on which Vietnamese users’ data are administered, within the territory of Vietnam. In addition, in respect of information systems critical to national security (defined vaguely as information systems which, when broken down or sabotaged, will affect national sovereignty, interests and security and seriously impact social order and safety), the owners of such information systems must store the personal information and critical data they have collected or created within Vietnam. If there is an obligation to provide any information outside of Vietnam, the information system owner must assess security levels as regulated by the MOPS or in accordance with other applicable legislation.

4 This Draft Cybersecurity Law has been widely criticised in Vietnam by the business community (including both Vietnamese and foreign business chambers/associations in Vietnam such as the Vietnam Chamber of Commerce and Industry (“VCCI”), American Chamber of Commerce and Asia Internet Coalition, *etc*) in that it imposes onerous measures and liabilities on telecom and Internet service providers. If the Draft Cybersecurity Law is promulgated as currently written, it would potentially impede the digital economy and the growth of telecom and Internet services in Vietnam as it prevents free flow of data.

3 No 86/2015/QH13.

4 “Data localisation requirements” may be broadly understood here as the prohibition against transfers of personal data without official approval or permit, even if data subjects have consented to the transfer.

B GENERAL LEGAL FRAMEWORK OF INTERNATIONAL DATA TRANSFERS

i Existing data privacy protections in national legislation

5 The right to privacy (including informational privacy and all forms of exchange of personal information) and confidentiality of information is a fundamental right recognised by the Constitution of Vietnam (Article 21). Currently, there is no single comprehensive legal document regulating data privacy in Vietnam, but there are a number of laws and regulations that have provisions to protect personal data privacy. These laws include the Civil Code,⁵ the Penal Code,⁶ the Law on Information Technology⁷ (“IT Law”), the Law on Telecommunications⁸ (“Telecom Law”), the Law on Network Information Security, the Law on Consumer Protection,⁹ the Law on E-Transactions,¹⁰ Decree 72 on Internet services and online information and Decree No 52/2013/ND-CP on e-commerce (“Decree 52”).

6 These laws provide a common key principle that the collection, processing and use of personal information must be consented to by the information owner,¹¹ and the use of such information must be in line with the purposes as notified and consented to. Transfer of personal information to a third party must be consented to by the information owner or at the request of a competent authority, or where the law provides otherwise. An information owner is entitled to request any organisation or individual storing their personal information in a network environment to check, correct or remove/delete such information; to supply to the information owner such information at their request; and to stop supplying their information to a third party at their request. The

5 No 91/2015/QH13.

6 No 100/2015/QH13.

7 No 67/2006/QH11.

8 No 41/2009/QH12.

9 No 59/2010/QH12.

10 No 51/2005/QH11.

11 For instance, Art 38 cl 2 of the Civil Code (Law No 91/2015/QH13) on “Right to Private Life, Personal Privacy and Family Privacy” provides that “the collection, storage, use, and publication of information related to the private life or personal privacy of an individual must have the consent of that person”.

person/organisation collecting, processing or using personal information of another person must also notify the data subject if it cannot comply with their request for technical or other reasons.

7 There is no data localisation requirement under the current legislation (*ie*, the Civil Code, the Penal Code, the IT Law, the Telecom Law, the Law on Network Information Security, the Law on Consumer Protection, the Law on E-Transactions, Decree 72 on Internet services and online information and Decree 52 on e-commerce). Data can be transferred cross-border to and from Vietnam if prior consent of the data subject is obtained. However, as discussed above, if the Draft Cybersecurity Law is promulgated as is, it will be the first legislation introducing data localisation requirements in Vietnam. At the time of writing this report, the Draft Cybersecurity Law is in the process of being reviewed by the National Assembly (*ie*, the Legislature of Vietnam). The National Assembly is scheduled to vote on this Draft Cybersecurity Law in the middle of 2018.

8 As with the data privacy rules, the definition of “personal information” under Vietnamese law is broadly provided in different pieces of legislation. Personal information is generally defined as information contributing to identifying a particular individual, including, among other things, name, date of birth, home address, phone number, medical information, identity card numbers, social insurance card numbers, credit or debit card numbers, information on personal payment transactions and other information that the individual wishes to keep confidential. The phrase “other information that the individual wishes to keep confidential”¹² is problematic in that it seems to give complete subjective discretion to the owners of the information to determine what is considered “personal information”.

9 While privacy rights are rather restrictive under statute, their enforcement as of now is extremely weak. Based on reports and this reporter’s discussion with the Ministry of Justice, it is uncommon for Vietnamese courts to handle privacy infringement claims.

12 Decree 52 Art 3(13).

ii *International engagement*

10 Vietnam ratified the International Covenant on Civil and Political Rights (“ICCPR”) on 24 September 1982, which entered into force for Vietnam on 24 December 1982. However, Vietnam has not taken action with regards to the Optional Protocol to the International Covenant on Civil and Political Rights. In addition, to date, Vietnam has entered into ten bilateral and multilateral free trade agreements (“FTAs”), some of which cover the provisions on transfer of personal data between Member States, such as the Trans-Pacific Partnership (“TPP”) which includes provisions for privacy and limitations on data localisation.

11 In theory, if there are conflicts between the provisions in the FTAs and the provisions in Vietnam’s domestic law, the provisions in the FTA could override the latter if one of the concerned parties is a foreign individual or entity. In particular, the Law on Promulgation of Legislative Documents specifies that “in case a Vietnam legislative document, other than the Constitution, and an international treaty of which the Socialist Republic of Vietnam is a member contain different regulations on the same issue, the international agreement shall apply”.¹³ Vietnam’s Civil Code also provides that “where an international treaty of which the Socialist Republic of Vietnam is a member regulates the rights and obligations of parties to civil relations involving a foreign element, such international treaty shall apply”. The Commercial Law¹⁴ reinforces that “the rights and obligations of enterprises with foreign-owned capital shall be determined in accordance with the law of Vietnam or international treaties of which the Socialist Republic of Vietnam is a member”. As the receiver of cross-border data transfers is an organisation or individual residing outside of Vietnam, the provisions in the FTA could override the restrictions on cross-border data transfers in Vietnam’s domestic law in cases of conflict.

12 Vietnam is a Member economy of the Asia-Pacific Economic Cooperation (“APEC”). However, Vietnam has not yet participated in the APEC Cross-border Privacy Enforcement Arrangement (“CPEA”).

13 Law on Promulgation of Legislative Documents (No 80/2015/QH13) Art 156(5).

14 No 36/2005/QH11.

According to a report published by APEC in January 2017, Vietnam is among six jurisdictions considering joining the APEC Cross-Border Privacy Rules (“CBPR”) system in the near future; however, the time when Vietnam will join the system was not reported.

13 With respect to Vietnam’s position on the Consultative Committee of the Council of Europe Convention 108, a meeting on cybercrime and data protection organised by the Franco-Vietnamese House of Law was held on 18–19 November 2009 in Hanoi, in which the Council of Europe contributed to a regional colloquium on the legal issues of the development of information and communication technologies. Participants from Vietnam, Cambodia, Laos and Thailand discussed amendments to the Penal Code which defined additional cyber-offences as well as further reforms that were envisaged for 2010 and 2011 to bring Vietnamese legislation in line with the Convention on Cybercrime. The event also created awareness of the need for data protection standards such as those of the Council of Europe’s Convention on the Protection of Personal Data (CETS 108 and 181). Except for such meeting, there does not appear to be any other publicly accessible information on Vietnam’s intention of admission to the Consultative Committee of the Council of Europe Convention 108.

14 Vietnam has not been recognised by the European Union as offering an adequate level of protection under Article 25(6) of Directive 95/46/EC, and has never submitted an application to that effect.

15 It is probable that as a result of the extraterritorial reach of the European General Data Protection Regulation (“GDPR”), European businesses which have subsidiaries in or business transactions concerning Vietnam will audit and implement their internal rules and procedures on data processing to comply with the GDPR, although this regulation is stricter than the data protection regulations in Vietnam.

iii Competent authorities in area of data protection and cross-border data transfers

16 As discussed above, there is no single comprehensive legal document regulating data protection in Vietnam, but there are a number

of laws and regulations that have provisions to protect personal data privacy.

17 The government bodies having the power to enforce data protection in Vietnam vary depending on the sector in which the data protection activities are involved. For example, the Ministry of Information and Communications (“MIC”) has the power to examine, inspect, settle complaints and denunciations, and handle data privacy violations in relation to the telecom, Internet and information technology (“IT”) sectors.¹⁵ The Vietnam e-Commerce and Information Technology Authority (“VECITA”), an organisation under the Ministry of Industry and Trade, has the power to handle data privacy violations in relation to the e-commerce sectors. VECITA is responsible for the state management of e-commerce activities in Vietnam, including guiding, licensing, monitoring and controlling the operation of e-commerce activities in Vietnam.¹⁶ The State Bank of Vietnam has the power to handle data privacy in the banking sector.¹⁷ The Ministry of Public Security has the power in relation to state secret protection, cybercrime, national security, social order and security. Finally, the investigation agencies of the People’s Police are empowered with wide authority to request the supply of information from organisations and individuals for investigation purposes.

15 Law on Telecommunications (No 41/2009/QH12) Art 9(2)(dd); Law on Information Technology (No 67/2006/QH11) Art 10(1); Decree No 72/2013/ND-CP on management, provision and use of Internet services and online information Art 39(1)(d); Law on Network Information Security (No 86/2015/QH13) Art 27(2)(a).

16 Decree 52 Arts 6(1), 77 and 78(5).

17 Law on Credit Institutions (No 47/2010/QH12) Art 159. In respect of the provision on data privacy, Art 14(3) of the Law on Credit Institutions provides that credit institutions and foreign bank branches shall not be permitted to provide information to any other organisation or individual about accounts, deposits, deposited assets or transactions of clients conducted at such credit institution or foreign bank branch, except when requested by a competent state body in accordance with law or when the client consents.

C DEFAULT POSITION, SCOPE AND TERRITORIAL EFFECT

i *Default position*

18 Based on the current legislation, there is no specific requirement with regards to international data transfers. International transfer is authorised when prior consent of the data subject is obtained, or when the transfer is made in accordance with the transferor's obligation under Vietnamese law (such as by court order or at the request of the competent authorities).

ii *Additional requirement to consent in banking sector*

19 In addition to the consent requirement, in the banking sector, data on client passwords and password users and other sensitive information (*ie*, data containing classified matter, information restricted to internal circulation within the entity, or information which the entity manages and which, if leaked, could have an adverse impact on the reputation, finances or activities of such entity) must be encrypted and protected when transferred, regardless of whether they are domestically or internationally transferred.¹⁸ This encryption requirement also applies to transfer of information classified as state secret.

20 There is no restriction on the location of the transferee of data.

iii *No difference in legal qualification between roles*

21 Vietnamese law does not distinguish the roles relating to data processing into data controller, processor or intermediaries. According to Vietnamese law, every person involved with the collection, process, use, storage, transfer, disclosure and publication of personal information needs to obtain prior consent from the data subject.¹⁹

18 Circular 31 Art 35(2).

19 Civil Code (No 91/2015/QH13) Art 38(2); Law on Information Technology (No 67/2006/QH11) Art 21(1); Law on Network Information Security (No 86/2015/QH13) Art 17(1)(a); Law on E-Transactions (No 51/2005/QH11)

(continued on the next page)

iv Exemption from obligation to obtain consent for certain types of data

22 Consent, however, may be exempted for the following:

- (a) collection of personal information already published on e-commerce websites;
- (b) collection of personal information for signing, modifying or performing purchase and sale contracts for goods and services;
- (c) collection of personal information for calculating prices or charges for use of information, products and services online; and
- (d) collection of personal information for performing other obligations in accordance with the law.

D LEGAL BASIS

23 The individual's consent is always necessary to transfer their data, irrespective of the implementation of data transfer mechanisms by the data exporter and/or the data importer. However, except for consent which is required to be obtained by e-commerce websites (for which the law clearly requires express consent from information owners in the form as prescribed by law), generally, other data privacy laws/regulations do not require a specific form in which the consent must be given. Consequently, it is unclear as to whether the consent must be express (*ie*, opt-in) or whether a notice and lack of objection would suffice.

24 If the data will be transferred electronically, the IT Law, which is the law governing the use of IT in a network environment (including providing, transmitting, collecting, processing and exchanging information via an information infrastructure, such as telecom networks, the Internet, computer networks and databases),²⁰ requires that the person collecting, processing or using personal information of another person must notify such person of the form, scope, place and purpose of the collection,

Art 46(2); Law on Consumer Protection (No 59/2010/QH12) Art 6(2)(b); Decree 52 Art 70(1); *etc.*

20 Law on Information Technology (No 67/2006/QH11) Arts 1, 4(3) and 4(4).

processing or use of their personal information. There is no statutory form or template for this notification.

25 In addition, the Law on Network Information Security further provides that if the information is collected, edited, used, stored, supplied, shared or dispersed in the network for “commercial purposes”, the organisation or individual handling the personal information must develop and publicise their own policies applicable to handling and protection of personal information.²¹

26 These notifications and privacy policies are not required to be notified to or approved by the regulator, government or public entity.

E DATA LOCALISATION²²

27 Based on the current legislation, Vietnam does not have data localisation requirements where the transfer of personal data is prohibited without official approval or permit, even if the data subjects have consented to the transfer.

28 However, data localisation requirements are introduced by the Draft Cybersecurity Law. If the Draft Cybersecurity Law is promulgated in its current version, foreign enterprises (companies incorporated outside of Vietnam), when providing telecom and Internet services in Vietnam, will be required to locate their servers on which Vietnamese users’ data are administered within the territory of Vietnam. It is unclear under the Draft Cybersecurity Law whether such foreign enterprises need to physically store and keep all the data in Vietnam or whether they can just keep a copy of the data in Vietnam for possible government inspection (while the data can also be transferred across the border to be processed and stored outside of Vietnam).

21 Law on Network Information Security (No 86/2015/QH13 Arts 3(17) and 16(3).

22 “Data localisation requirements” may be broadly understood here as the prohibition against transfers of personal data without official approval or permit, even if the data subjects have consented to the transfer.

29 In addition, the Draft Cybersecurity Law further introduces that in respect of information systems critical to national security (defined vaguely as information systems which, when broken down or sabotaged, will affect national sovereignty, interests and security and seriously impact social order and safety), the owner of such information systems must store the personal information and critical data they have collected or created within Vietnam. If there is an obligation to provide any information outside of Vietnam, the information system owner must assess the security levels as regulated by the MOPS or in accordance with other applicable legislation. However, the Draft Cybersecurity Law does not provide the definition of “critical data”, details on the assessment procedure, or the criteria to establish whether the security level is sufficient for transferring the data outside of Vietnam.

30 According to the Draft Cybersecurity Law, there is no exception to these data localisation requirements.

31 The Draft Cybersecurity Law is currently drafted to be applicable to Vietnamese agencies, organisations and citizens, and foreign organisations and citizens, directly involved in or connected to activities related to cyberspace (which is defined as the global network of information technology infrastructure, including the Internet, telecom networks, computer systems, and information processing and control systems, which is a special environment where humans perform social activities without being limited by space and time) and the protection of cybersecurity of Vietnam.

F DATA TRANSFER MECHANISMS

i *Preliminary issues*

32 Vietnamese law does not specifically distinguish between the transfer of data within or outside of Vietnam. The rules for the transfer of personal information both within and outside Vietnam are the same. That is, organisations and individuals must refrain from providing, sharing or spreading to a third party personal information they have collected, accessed or controlled, unless they obtain the consent of the data owners or it is at the request of the proper state agencies.

33 The law generally does not require a specific form in which consent must be given. It is unclear whether consent must be affirmative or if implied consent is sufficient. However, Vietnam is a very formalistic jurisdiction. Thus, the recommended best practice is clear, affirmative opt-in consent, and a signature on paper is preferable. However, for electronic transactions, where it is impractical to obtain a signature on paper, consent may be obtained by a click-to-accept mechanism.

34 The person collecting, processing or using personal information of another person may only use and store the collected information for a certain time period as stipulated by law or as agreed upon by the data subject, and may not supply, transfer or disclose the information to any third party unless otherwise stipulated by law or agreed to by such person.

35 Vietnamese law does not specifically require transfer instruments that are compatible or promote interoperability between countries. In general, the law does not impose an obligation on the data exporter to ensure that the recipient is bound by legally enforceable obligations regarding the protection of the transferred data, except in certain specific industries like banking. Under the banking laws/regulations, there must be a written agreement before information is exchanged with any outside parties (regardless of whether the transfer is within or outside of Vietnam), specifying the legal responsibilities and obligations of the parties involved, including terms and conditions on dealing with breaches by the third party and its liability to pay compensation for loss and damage caused by breaches.²³

36 The law generally provides that an individual shall be entitled to claim compensation for loss caused by a breach during the supply of personal information. However, it is unclear whether the data exporter must remain liable in the case of a breach by a data importer overseas.

23 Circular 31 Art 30(2).

ii *“Adequacy findings” and white lists*

37 Vietnamese law does not specifically require that data must only be transferred to jurisdictions that have laws establishing adequate or comparable data protection standards. A data exporter is free to assess the level of protection awarded in the country of destination. In general, there is no “black list” for jurisdictions (inside or outside Asia) which do not establish adequate or comparable data protection standards.

iii *Consent as exception to existence of privacy safeguards overseas*

38 Vietnamese law does not have requirements on privacy safeguards in the country of destination. However, the data importer/processor overseas must comply with the data protection rules under Vietnamese law when processing personal information of Vietnamese data subjects overseas. The data importer/processor overseas cannot obtain consent from the Vietnamese data subject to waive its obligations under the Vietnamese data protection rules.

iv *Other one-off exceptions*

39 Vietnamese law does not have requirements for privacy safeguards in the country of destination.

40 A data exporter cannot transfer personal information of data subjects in Vietnam to another person unless otherwise provided for by Vietnamese law or consented to by the data subject. The law does not provide explicit exceptions for cases where such information is necessary for the performance of a contract requested by the data subject or legal proceeding outside of Vietnam. It is worth noting that a foreign court’s order requiring the data exporter to reveal personal information of data subjects in Vietnam requires recognition by a Vietnamese court through

a formal procedure pursuant to the Civil Proceedings Code before taking effect.²⁴

v *Contracts*

41 As discussed above, except for certain specific industries like banking, it is not compulsory for a data exporter to conclude a contract with the data importer, irrespective of the status of the recipient (data intermediary, controller, *etc*). Other guarantees (CBPR certification, Binding Corporate Rules, *etc*) are also not compulsory.

42 Under the banking laws/regulations, there must be a written agreement before information is exchanged with any third parties (regardless of whether the transfer is within or outside of Vietnam) The agreement for transfer of information between the data exporter and the data importer must specify the legal responsibilities and obligations of the parties involved, including terms and conditions on dealing with breaches by the data importer and its liability to pay compensation for loss and damage caused by breaches.²⁵ It is not compulsory to include a third-party beneficiary clause for the benefit of the data subjects. There are no standard contractual clauses for this type of agreement.

vi *CBPR*

43 As discussed above, Vietnam has not yet participated in the APEC CPEA. According to a report published by APEC in January 2017, Vietnam is among six jurisdictions considering joining the APEC CBPR system in the near future; however, the time when Vietnam will join the system was not reported.

24 Principally, foreign court orders or judgments are generally unenforceable in Vietnam unless there is a judicial decision recognition treaty with the relevant country or the Vietnamese court enforces the foreign court's order/judgment on a reciprocal case-by-case basis (Art 423(1) of the Civil Proceedings Code (No 92/2015/QH13)).

25 Circular 31 Art 30(2).

44 As Vietnam does not have a comprehensive data privacy protection law, it is cautioned that there are various unresolved issues that need to be addressed before it can join the CBPR. The issues include, for example, which government agency would lead the application process or be responsible for enforcement of the CBPR, and how to structure the certification process to ensure its scalability to companies of all sizes. To address these issues and others, Vietnam may need to bring in a number of international experts, who have been significantly involved in either the creation or implementation of the CBPR system, or have other relevant experience in the governance of cross-border data flows, organisational accountability and data protection management, before the adoption of regulations to allow for such certification.

vii *Certification, trustmarks and privacy seals*

45 Certification, trustmarks and privacy seals are currently not compulsory under Vietnamese law.

viii *Other data transfer instruments*

46 Currently, there are no other accountability instruments or data transfer mechanisms compulsorily required under Vietnamese law.

G INTERNATIONAL CO-OPERATION BETWEEN PUBLIC AUTHORITIES WITH SECTORAL RESPONSIBILITIES IN DATA PROTECTION

i *Co-operation with foreign authorities in areas other than enforcement*

47 The law currently includes provisions that enable the Vietnamese authorities to develop operational co-operation with the authorities in other countries in this area of law.

48 For example, Article 6 of the Law on Network Information Security provides that:

1. International cooperation on network information security should abide by the principles as follows:

- a) respecting the independence, sovereignty and territorial integrity of countries without intervention in internal affairs of the others, for equality and mutual benefits;
 - b) complying with Vietnam laws and international treaties to which the Socialist Republic of Vietnam is a state member.
2. Contents of international cooperation on network information security include:
- a) international cooperation on research and application of science, techniques and engineering of network information security;
 - b) international cooperation in prevention and fighting illegal acts in relation to network information security, and against the abuse of information networks for terrorist acts;
 - c) other international cooperation on network information security.

49 The Draft Cybersecurity Law also includes provisions that enable the privacy enforcement authority (“PEA”) to develop operational co-operation with the PEAs in other countries. In particular, the Draft Cybersecurity Law states that:

- 1. Vietnamese organisations and individuals shall cooperate with foreign organisations and individuals or international organisations on cybersecurity in the principles of respecting national independence and sovereignty, non-interference in the internal affairs of each other, equality and mutual interests.
- 2. The contents of international cooperation on cybersecurity include:
 - a) research on and analyses of cybersecurity trends;
 - b) mechanisms and policies for further cooperation between Vietnamese organisations or individuals and foreign organisations or individuals or international organisations operating in cybersecurity;
 - c) sharing of information and experience, and support in training, equipment and technology for cybersecurity assurance;
 - d) prevention of and fighting against cybercrimes and acts prejudicial to cybersecurity, and the prevention of cybersecurity threats;
 - e) training and development of cybersecurity human resources;
 - f) organisation of international workshops, conferences and forums on cybersecurity;
 - g) signing, entry into and performance of bilateral and multilateral international treaties and participation in regional and international organisations on cybersecurity; and

- h) execution of international cooperation programs and projects on cybersecurity.

50 However, the Vietnamese authorities do not appear to have any bilateral or multilateral arrangements with the authorities of other jurisdictions to co-operate in the implementation of privacy laws.

51 In general, before the Vietnamese authorities adopt regulatory guidance or when making decisions that have a major impact on individuals and companies operating in Vietnam, they usually organise public consultations on the draft legislation and are open to comments from experts, businesses and organisations for insight into industry perspective and internal practice. However, the authorities do not have any statutory obligation to ensure regional or international consistency in their decision-making process, unless Vietnam is bound by regional or international commitments for such consistency.

ii *Enforcement of cross-border transfer restrictions*

52 Breaches of provisions on international data transfers or data localisation, depending on the nature and level of violation, may be subject to disciplinary or administrative treatment or penal proceedings, and to payment for any damage under current laws. However, it is worth noting that while the Vietnamese data protection and privacy rules are rather restrictive under statute, their enforcement as of now is extremely weak. Based on reports and this reporter's discussion with the Ministry of Justice, it is uncommon for the Vietnamese courts to handle privacy infringement claims.

53 There are small administrative penalties that might apply (the local equivalent of about US\$450 to US\$900) for an act of collecting, processing, using and transferring personal data without proper consent.

54 A breach of cross-border data transfer may also be subject to criminal sanction if:

- (a) the transfer infringes secret information, mail, telephone, or telegraph privacy, or other means of private information exchange, for which the offender has already been disciplined or assessed with administrative penalty; or

- (b) the transfer is associated with trading, exchanging, giving, changing, or publishing lawfully private information of an organisation or individual on a computer or telecom network without the consent of the information owner, provided that the offender earns an illegal profit of from VND50,000,000 to under VND200,000,000 (approximately US\$900 to US\$8,800) or causes property damage of from VND100,000,000 to under VND500,000,000 (approximately US\$4,400 to under US\$22,000) or damages the reputation of an organisation or individual.

55 The potential criminal sanctions range from a fine of VND20,000,000 to VND200,000,000 (approximately US\$880 to US\$8,800), a penalty of up to three years community sentence, being prohibited from holding certain positions for up to five years and imprisonment for up to three years. However, imprisonment penalties may be assessed only if: the offence is committed by an organised group; the offence involves abuse of the offender's position or power; the offence has been committed more than once; the obtained information is disclosed and affects another person's dignity or reputation; or the offence results in the suicide of the victim.

56 Relatedly, with regard to the risk of civil claims, it is uncommon for the Vietnamese courts to handle privacy infringement claims. The Vietnamese courts are limited to actual and direct losses, which often are out-of-pocket costs. Losses which are more difficult to prove are not usually awarded. A claimant who has suffered from a violation of data protection and privacy laws would need to prove their losses, which is difficult to do in practice. Given various factors, including the difficulties with litigation in Vietnam, a common scenario in many contexts is that would-be claimants might just ask for an apology or some form of negotiated monetary settlement.

57 The inspectorate division of an authority may initiate an investigation into a violation of the law or, more frequently, conduct an investigation when it is notified either by other government bodies, private sectors or news reports with high public visibility. However, to the best of this reporter's knowledge, no Vietnamese authority has ever taken action against a (national or foreign) controller based on the

conditions in which local data had been transferred to another jurisdiction.

iii *International enforcement by Vietnamese authorities*

58 Vietnam is a member of Interpol (International Criminal Police Organization), an international organisation facilitating international police co-operation. Interpol's National Central Bureau ("NCB") for Vietnam, which also serves as the MOPS's Department of Foreign Relations, is the primary law enforcement platform for Vietnamese police investigations requiring co-operation with other countries.

59 The NCB's principal responsibilities include:

- (a) working with domestic, regional and international partners in developing events and programmes to boost Vietnam's ability to identify and prevent transnational crime;
- (b) providing intelligence support to domestic law enforcement units when investigations require global outreach;
- (c) co-ordinating the arrest and extradition of fugitives located in Vietnam, and of Vietnamese fugitives located in Interpol member countries; and
- (d) working with all member countries for matters relating to mutual legal assistance on criminal matters and extradition.

60 Vietnamese domestic law currently does not include provisions for any of the following: transfer of complaints to the authorities in other jurisdictions; disclosure to the authorities in other jurisdictions of information obtained in investigations; assisting other authorities in cross-border investigations; or a prohibition on providing information to other enforcement authorities.

61 The Vietnamese authorities have not yet participated in any of the existing enforcement co-operation networks or arrangements on data protection and privacy (*eg*, GPEN, GPEN Alert and UCENet).

62 Vietnam does not have any bilateral arrangements with the PEAs of other countries to co-operate in the enforcement of privacy laws. However, Vietnam has co-operated with a number of PEAs in other

countries, including those from the US, the UK and China, in order to exchange intelligence and information and jointly investigate cases relating to cybercrime. Vietnam has also co-operated with its international counterparts in training and sending its officers to meetings, conferences and training courses.

ISBN 978-981-11-7311-0



9 789811 173110