Where are we now with data protection law in China?

Until recently, China’s data privacy framework consisted only of a patchwork of fragmented rules found in sectoral, insurance and sector-specific regulations. While the reasons of obvious forms of personal data in Appendix A of the Guidelines include medical records, social and public interests, law enforcement or key infrastructure, etc.

The PI Security Specification states that an incident notification must explain:

- the measures taken or to be taken in response to the incident;
- the impact and potential impact of the incident; and
- the confidentiality. This includes an obligation to implement technical measures to monitor and record data processing activities.

In addition to the requirements to keep personal data secure, the Cyber Security Law also contains provisions on the transfer of personal data, the collection of personal data and the retention of personal data.

Accordingly, the data privacy provisions in the Cyber Security Law will apply to all organisations for China that provide services over the internet or another information network. Internal networks and systems might potentially be caught as well, but this is less clear.

**Data protection obligations under the Cyber Security Law**

The Cyber Security Law imposes data privacy obligations on network operators. The term ‘network operator’ includes both owners and administrators of a network as well as network service providers.

A ‘network’ is defined as any system that consists of computers or other information terminals, and related equipment for collecting, storing, transmitting, exchanging and processing information.

Accordingly, the data privacy provisions in the Cyber Security Law will apply to all organisations for China that provide services over the internet or another information network. Internal networks and systems might potentially be caught as well, but this is less clear.

**Definitions of personal data**

The Cyber Security Law defines personal data or information that identifies a natural person either by itself or in combination with other information. The term includes a person’s name, address, telephone number, date of birth, identity card number and biometric identifiers.

**Data collection and processing**

Network operators are prohibited from collecting personal data that is not relevant to the services that they offer. It is unclear how strictly this prohibition will be enforced.

Before collecting personal data from an individual (the data subject), a network operator is required to inform the individual of the purposes, means and scope of the collection and use of their data, and obtain their consent for collection. Any processing of personal data must be done in accordance with the scope of those consents. The purpose limitations under the Cyber Security Law are not entirely consistent.

It is unclear whether the above requirements are intended to apply to employees and business contacts.

**Storage and security**

The Cyber Security Law requires network operators to keep personal data, except in cases specified by the measures. This includes an obligation to implement technical measures to monitor and record data processing activities.

Network operators are also required to back up and encrypt so-called ‘important data’, and to store operations logs for at least six months. The Security Assessment Measures define ‘important data’ as data that is closely related to national security, economic development and social and public interests. (There is an in-depth discussion of the Cyber Security Law here).

On 30 August 2017, the National Information Security Standardisation Technical Committee (TC260) released the second draft of the non-binding Guidelines for Cross-Border Data Transfer Security Assessment (the Guidelines for Cross-Border Data Transfers). These Guidelines provide detailed guidance on the criteria for cross-border transfers of data, and are based on the corresponding provisions of the Cyber Security Law.

**Incident notification**

The PI Security Specification states that an incident notification must explain:

- the nature and impact of the incident;
- the measures taken or to be taken in response;
- the practical recommendations for data subjects to minimise the impact of the incident;
- data subjects’ rights and remedies.

**Designated personnel**

The Cyber Security Law requires network operators to appoint personnel responsible for network security as part of their internal security management systems. While the law falls short of requiring operators to appoint a specific data protection officer, the PI Security Specification does however provide that operators are expected to designate a person or group to manage personal data.

Under the Security Assessment Measures and the PI Security Specification, if an organisation has more than 200 personnel and its main business involves processing of personal data, or if an organisation has more than 10,000 personnel and its main business involves processing of important data, it should establish a department with dedicated staff to handle personal data security.

**Transfer of data**

**Informed consent**

Under the Cyber Security Law, it is necessary to obtain the informed consent of data subjects to transfer or disclose any of the personal data to a third party (whether within or outside the country).

Under the Security Assessment Measures, to obtain informed consent to a transfer of personal data.
of personal data, the network operator must first notify the Data subject of:

- the type of personal data being transferred (to allow individuals to understand what
  personal data is involved);
- the purpose and scope of the transfer;
- the recipient and the country to which the data will be transferred.

In certain circumstances, consent may be implied where the Data subject's actions, such
as making international telephone calls, sending international emails or instant messages,
and conducting international transactions even across the internet (the Guidelines for Cross-Border Data Transfer), do not need to be considered a security assessment as an
annual basis before transferring any personal data out of China. The security assessment
must be carried out by an independent third-party professional organization that has
been approved after filing the security assessment report with the designated authority (to
be determined by the requirements established above).

Another criterion for the security assessment is whether the transfer includes any 'important
data', i.e. data related to national security, economic development and societal and public
interests.

The inclusion of 'important data' is not a decisive factor against authorising the data export.
It is one factor among several, which could potentially therefore be offset by, for example,
higher security provisions. (All 'important data' must be encrypted at all times in any event.)

The main consideration for the security assessment when transferring 'important data' is the
impact on national security, economic development and societal and public interests, so
that the security assessment is a balance between these factors. If the security assessment
does not meet the relevant threshold, the relevant business function cannot be fulfilled.

The Guidelines set out a scoring system to assess the impact of the data transfer that
emphasises the inter-relationship between the various factors in the security assessment
(Appendix B). While detailed in terms of identifying the various considerations to be taken
account of, the scoring system nevertheless bears a general and broad concept.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines set out a scoring system to assess the impact of the data transfer that
emphasises the inter-relationship between the various factors in the security assessment
(Appendix B). While detailed in terms of identifying the various considerations to be taken
account of, the scoring system nevertheless bears a general and broad concept.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.

The Guidelines also introduce the use of desensitisation measures to reduce the impact of
the data transfer in accordance with the relevant thresholds described above. While specific about what these measures should consist of, the CAC is presently referring to techniques such as
randomisation, some combination of techniques that do not fully conceal the data transfer,
or techniques that are not available.
Data localisation is not a new concept in China. Existing data localisation provisions are contained in sectoral regulations in the banking, insurance and healthcare industries:

- Under a Notice of the People's Bank of China, the PI Security Specification (effective as of January 2018), financial personal data relating to Chinese citizens collected within China is required to be processed, monitored and analysed within China. Banks in China are not permitted to transfer the personal financial information of Chinese clients to any other country without the approval of the PI Security Specification. Furthermore, personal data that is collected within China by health and family planning institutions in China is also required to be processed, monitored and analysed within China. This is because banks and health and family planning institutions are required to maintain the confidentiality of the personal data of Chinese citizens.

- The China Insurance Regulatory Commission has issued a number of regulations requiring financial and financial data of insurance companies to be stored within China. Insurance companies are also required to have independent data management systems and ensure that such systems are fully compliant with the PI Security Specification.

- The National Health and Family Planning Commission's Administrative Measures on Management of Population and Health Information (promulgated on 1 May 2016) require the storage of personal data by health and family planning institutions in China. These institutions are also prohibited from providing medical information or services outside of China.

- In addition, the recently released Draft Measures for the Information Technology Management of Insurance and Funds Operators (effective 5 May 2017) require data localisation obligations applicable to insurance and funds operators.

**Data protection obligations under the PI Security Specification**

The PI Security Specification requires data controllers to conduct an impact assessment at least once a year in conjunction with any major change to their operating model, information systems or following a data security incident. This requirement is more limited than those under the GDPR, where impact assessments are generally required for each large-scale data processing project.

The impact assessment should consider, among other things, whether the organisation's data processing activities have an adverse impact on the fundamental rights and interests of data subjects, including their freedom of expression or religion, or could lead to discriminatory treatment. Where matters are to be reviewed include the effects of information security measures, the risk that a concentration of anonymised and de-sensitised personal data might lead to identification and the adverse impact of transfers of personal data.

**Sensitive personal data**

The PI Security Specification distinguishes between general and sensitive personal data. Sensitive personal data includes personal data defined as personal data that, if disclosed or illegally processed might endanger personal and property security, cause personal injury, or have psychological, physical or emotional psychological or physical health and educational treatment, etc. Sensitive personal data may include personal ID numbers, bank account numbers, personal communications, credit records, personal data and health data, and are considered to be data that may impact on children under the age of 14.

The data subject's express consent in writing or through other affirmative action is required to collect sensitive personal data (e.g. age). Consent must be kept (transferred and accessible) for a period of at least 15 years after the last collection of the data. Following the collection of sensitive personal data that is not sensitive (e.g., case reports), it is required that the data controller ensures data security.

**New rights of Data Subjects**

In addition to the data access and correction rights granted under various laws and regulations, the PI Security Specification introduces the first time ever the right to data portability for the individual rights under GDPR.

The data controller shall have the right to ask the data controller to ensure all users and to secure personal data of the data controller to the data controller's standard legal obligations or an agreement with the data subject (comparable to the GDPR (right to be forgotten)). The same right extends to information in the possession of data processors.

**Automated decision making**

An appeal mechanism must be provided in relation to automated decisions that directly affect the rights and interests of data subjects (e.g. the drawing up of the approaches under the GDPR with the right to be subject to automated decision making). The example given in the specification is automated credit rating decisions and screenings of job applicants.

**Data pseudonymisation**

Data controllers are required to conduct an impact assessment before engaging a third party to pseudonymise data, to ensure that the data processor is able to ensure data security. Data controllers are required to conduct oversight of the processor, including by auditing the processor's activities.

**Provision of data**

Data processors also have a number of direct obligations under the PI Security Specification, including a requirement to strictly follow the data controller's instructions, obtain its authorisation before engaging a sub-processor and to delete all personal data at the end of the contract period.

**Incident handling**

Organisations should formulate a contingency plan for data incident and ensure incident response training and contingency drills at least once a year.

**Data protection obligations under other PRC laws and regulations**

Telecommunications and internet information service providers are subject to additional personal data protection obligations under the PRC on Protecting the Personal Information of Telecommunication and Internet Users (effective as of July 2015).

Telecommunications and internet information service providers are required to establish a user complaint mechanism and right to complaint concerning personal data protection within 15 days. Users may also require information about the channels through which they may seek redress and make complaints to their personal data.

When telecommunications and internet information service providers transfer personal data to other service entities (e.g., for market research or technical services), they may require the service provider to ensure the protection of the transferred personal data. They are also required to have in place the procedures to verify the authenticity and integrity of the transferred personal data.

**E-Commerce Law**

Under the e-Commerce Law, while which will come into effect on 1 January 2019, e-commerce operators are required to delete a user's personal data if they no longer have a legal or economic basis for collecting and using the data (e.g., the terms and conditions of the site alter significantly).

In addition, the obligations on all network operators under the Cyber Security Law, -
commerce providers must implement specific technical measures to ensure the security and normal operation of an e-commerce network and to respond effectively to cyber incidents. They must also prepare emergency response plans to manage incidents and report the incidents to the competent authority.

Direct marketing

The Consumer Protection Law (revised with effect on 14 March 2014) prohibits businesses from sending commercial information to consumers that they have not requested or consented to receiving, or where they have expressly objected to receiving the commercial information.

The Measures for the Administration of Email Services (effective 30 March 2006) prohibit the sending of any email containing commercial advertisements without (i) the recipient’s clear consent, and (ii) including the word ‘Ad’ or the Chinese word for ‘advertisement’ in the email subject. If a recipient subsequently opts out from receiving commercial advertisements, the sender must stop sending them.

Penalties under the Cyber Security Law

Penalties for infringements of the core data protection provisions of the Cyber Security Law may include a fine of up to five times the amount of unlawful gains or a fine of up to RMB 100,000. Persons in charge of data protection compliance within an organisation, and other responsible individuals, may be separately subject to a fine of between RMB 10,000 and 100,000, or between RMB 50,000 and 500,000 for serious cases.

The Interpretations of the Supreme People’s Court and the Supreme People’s Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens’ Personal Information (effective 1 June 2018) set out certain circumstances in which the unauthorised collection, transfer or receipt of personal data will constitute a criminal offence under the PRC Criminal Law, and the associated penalties. For example, the establishment of websites or communication groups for obtaining, selling or transferring personal data can be punished upon conviction by a fine of up to five times the illegal proceeds, and imprisonment for up to three years. A person convicted of illegally obtaining personal data concerning communication records, health information or credit or asset information can be punished by a fine of up to five times the illegal proceeds and imprisonment for up to seven years.