

The Sedona Conference WG11 Brainstorming Group Outline - Proactive Privacy and Security Governance: Complying with Global Data Privacy and Security Laws and Regulations (Sept. 2019)



Copyright 2019, The Sedona Conference.
All rights reserved.

Proactive Privacy and Data Security Governance: Complying With Global Privacy and Data Security Laws (September 2019)

Brainstorming Group:

Drew Sorrell (Brainstorming Group Leader)

Jami Mills Vibbert (Brainstorm Group Leader and Steering
Committee Liaison)

Jake Bernstein

Peggy Bodin

Chris Cronin

Sheryl Falk

Louise Rains Gomez

Ben Hawksworth

Jerami Kemnitz

Wendy P. King

Wayne Matus

Bradley L. Mirkin

Tim Noonan

Adam Rubinger

Mengyi Xu

John Yanchunis

Attached is the outline of the WG11 Brainstorming Group on Proactive Privacy and Data Security Governance for presentation at the WG11 Midyear Meeting in Montreal on Sept. 18-19, 2019. The outline (in this form) was previously presented to the entire Working Group via email prior to, and to a subset of the membership in person at, the WG11 Meeting following the 11th Annual Sedona Conference International Programme on Cross-Border Data Transfers and Data Protection Laws in Hong Kong, on June 20, 2019. During the Hong Kong meeting, the Brainstorming Group received feedback on the outline, which included agreement by the participants that some work product in this vein would be beneficial. The form of that work product, however, was the subject of much discussion during that session.

As a result of that holistic feedback, the Brainstorming Group reconvened. We focused primarily on brainstorming how the work product may better serve the needs of WG11 and the public at large, while still meeting Sedona's mission. We did not believe that there was a consensus from the feedback in Hong Kong on the best and appropriate subject matter and format of any work product to suggest to a drafting team. We plan to focus on these overarching issues during our presentation of the work product at the Midyear Meeting in Montreal: (1) whether we should revise the current outline to create a consolidated hybrid, risk-adjusted approach that incorporates concepts from the approaches currently outlined; (2) whether privacy and data security can and should be discussed in one document; and (3) scope.

For those members not attending the Montreal Meeting, we of course welcome your feedback on the outline and the noted overarching issues, too.

PROACTIVE PRIVACY AND DATA SECURITY GOVERNANCE: COMPLYING WITH GLOBAL PRIVACY AND DATA SECURITY LAWS

I. INTENDED AUDIENCE

A. Who?

1. In-house (General Counsel, Privacy, or Compliance functions) and others responsible for drafting and implementing companies' data privacy and security governance frameworks; and
2. Outside Counsel tasked with advising in-house contacts.
3. Although not the primary audience, the draft could be useful for:
 - i. InfoSec and in-house data security teams;
 - ii. Cybersecurity firms;
 - iii. HR and Communications; and
 - iv. Third party service providers.

B. Why do they need it?

- b. To help create consistent and defensible best practices that are understandable and can be scaled for large or small organizations and diverse business models.

C. Why and how this issue is of interest?

1. Uncertainty exists in initial and overall approach to managing and complying with the deluge of global data privacy and security laws - which is particularly challenging given the ever-changing technology used by organizations, the mobility of employees, the ways in which organizations relate to their clients/customers and vendors and the pace at which change is occurring.
2. What would be helpful is a roadmap to tackle data privacy and security compliance that could be scaled or adapted to any organization. Key components of this roadmap could include:
 - (a) Instructions for helping organizations understand their own business - how they receive or collect, utilize, share, transfer, retain and dispose of data within and outside the organization, across and within borders. This may include:

- (i) Strategic considerations for attacking the problem;
- (ii) Process guides for developing approaches;
- (iii) Overviews of common data repositories, systems, applications; and
- (iv) Exemplar workflows, maps and other templates.

(b) Advice to help organizations identify and understand the applicable data privacy and security requirements and drivers - which includes laws, regulations, ethical obligations as well as industry standards, contractual requirements, internal policies/procedures and other authoritative sources. This will not be a summary of laws, regulations, obligations, and standards - instead it will provide insight into how to determine which requirements exist, why they may be applicable, and how to digest and prioritize them.

(c) Practical guidance to help map the requirements identified in (b) to the business needs outlined in (c) to create and maintain a data privacy and security program that will withstand the dynamic business and legal environmental changes. This could include a decision-tree or high level examples of policies/frameworks, or examples of tools that exist or could be created to help track and monitor the decisions that are made.

3. Specific issues to address with various approaches:

- (a) Purchases or merging of companies would affect the entire company, and
- (b) Systems and processes common to all approaches.

D. Other Considerations

1. The drafting team may decide to provide examples of analysis or work product to help organizations apply the document's recommendations. The matrix provided in Appendix A is one such example. The risk register in Appendix A addresses two of the four concepts described in this document; the "one program to rule them all" and "reasonableness" approaches.

2. Avoid developing work product that contains a complex and long-winded analysis. As an in-house lawyer, we are often working at a pace that requires clear and concise guidance that can be adapted and repurposed.

3. Most Sedona work product includes a summary of general governing principles in the relevant areas. We should determine whether the principle/commentary structure would help distill our thoughts.

4. How can we develop and express best practices in a way that will be meaningful for organizations of different sizes (not just in size but with differing resources or risk tolerance), with different business models (b2b vs consumer-facing) and with different levels of information governance or information technology maturity.

II. DIFFERENT APPROACHES TO PROACTIVE GOVERNANCE

As a brainstorming group, we suggested several approaches that may be helpful to a company developing a proactive privacy and data security program. While we do not believe there is a one-size-fits-all approach, we provide the following as approaches that a drafting team could develop, with thoughts about what the approach looks like and what types of organizations may benefit from each approach.

A. Global Approach

1. Legal regimes

(a) Rather than focus on any specific compliance regime, organizations should review all applicable or regulations and formulate a single vision for their security and privacy program.

(b) Our task will include the creation of a holistic outline of concepts that all security and privacy regulations share. For example, there is, by and large, a clear focus on “reasonable security practices.” We should explore that concept and provide assistance for practitioners wondering what exactly this means. Another example is to leverage existing comparisons of the key components of the GDPR and CCPA to create an outline of what is needed.

(c) Another factor is how this approach will help in responding to assessments/audits (for organizations who provide services to others) and initiating assessments/audits of third party services providers.

(d) One problem to address is the “tail wagging the dog”. A small country could, regardless of footprint, set security and privacy rules for the global enterprise.

(e) This approach is “one size fits all”. We will explore whether to structure this by geographical regions or in another way. Questions to consider include:

(i) Can we categorize or “bucket”, the rules.

(a) Identify existing privacy/security rules and regulations

(b) Compare and review these regulations to be grouped

(ii) What problems will this approach solve?

(iii) What problems will remain (or be exacerbated) by this approach?

(iv) Who should (or can) bear responsibility for managing this approach within the organization?

2. *Systems/Data*

(a) Generally, we should counsel against segregation of networks and data in order to comply with the strictest rules only where those rules apply. Complexity is the enemy of effectiveness when it comes to security and without effective security, you cannot have effective privacy controls.

(b) In this landscape where we can anticipate more change is coming (federal US privacy regulation?) and future interpretation of existing regulations are there benefits to a baseline program which complies with most existing privacy regulations (or a reasonableness approach/standard) but allows for “add-ons” as regulations change/are interpreted and new ones created?

(i) What (if anything) can be done to create a “baseline” program which better positions companies for what’s to come and some of the unknown – is this possible?

3. *Pros/Cons of the Global Approach*

(a) *Pros:*

- (i) Provides a consistent framework
- (ii) Easier to integrate with other organizational efforts
- (iii) Potential savings through cost efficiencies
- (iv) Allows for consistent branding/messaging
- (v) Allows for an easier conversation about issues/events because everyone is speaking from the same place

(b) *Cons:*

- (i) Potential cost for extra rigor which is not required/necessary
- (ii) May work for larger organizations because they have more control over their business and influence over business partners

(iii) Challenging to implement because of potential conflicts in laws

(iv) Extra effort required to address “push-back” from clients, customers, service providers because generalized approach does not work for other organizations

(v) Potential loss of sales (Some multinational companies are pushing down the privacy requirements of jurisdiction x onto customers in jurisdiction y via terms and conditions. Government customers often cannot bind themselves to the laws of another country. Private companies will also require one-off negotiations if there is a conflict or will have to purchase a different solution.)

B. Jurisdiction-specific approach

1. The Drafting Group should evaluate the feasibility of creating an analytical and/or graphical representation of the spectrum of privacy/data security regimes around the world.

(a) The Drafting Group should first consider whether similar analyses currently exist.

(b) If so, are they adequate in laying out the complexity of the landscape and in providing practitioners with the appropriate tool to think through the compliance-design issue?

(c) If not, the Drafting Group should endeavor to group the current data privacy regimes in some coherent manner (GDPR-like/Omnibus, non-GDPR like, primarily sector-by-sector, by definition of personal information, by scope of coverage, by enforcement authority, by rights afforded to data subjects— e.g., Right to be Forgotten, Right to Notice, Right to Opt-Out, No Discrimination, Security, Access, Portability, by availability of additional guidance, etc.).

2. The Drafting Group should consider creating a process-based flow chart for compliance design, highlighting the role for each of the constituencies, the key questions for each stage and constituency, taking into account the unique requirements that each type of regulatory regime demands.

3. The Drafting Group should consider creating a checklist of key questions to ask the various constituencies when devising the governance framework (whether it is to revise a preexisting data governance plan or to draft one from scratch); note that some questions would be unique to categories of regulatory regimes identified in b. i.

4. Alternatively, the Drafting Group could consider simply outline the key elements of a data governance plan that is applicable to one or more categories of regulatory regimes, with emphasis placed on elements that differ. The Drafting Group should consider including in the final delivery a sample/template data governance plan for one or more categories.

5. The Drafting Group should deliberate on whether it is advisable to craft the deliverable, or part of it, into a dynamic tool, in light of the fast-changing nature of the field. The Drafting Group should think about how to ensure that the work product remains relevant despite likely changes in data governance regimes and how it can exist in a form that could be easily updated on a timely basis.

6. Guiding vectors for the analytical framework:

(a) BUSINESS LOCATION (includes all political subdivisions, such as states, provinces, and regions)

- (i) Where is the global company headquarter?
- (ii) Is the global company physically present other than where headquartered?
- (iii) Does the global company do business (solicit, regularly transact business) other than where headquartered or physically present?

(b) DATA LOCATION

- (i) Identify each location where the global company collects, sells, shares, buys, uses, transfers or stores personal/corporate data?

(c) DATA SUBJECTS

- (i) Where do the data subjects for personal data reside or have citizenship?

(d) DATA FUNCTIONS

- (i) What does the company do with the data? (Are they a processor, controller, buyer, seller, aggregator, user, collector etc.?)
 - How does the data flow within the region and outside of the region?

(e) DATA SYSTEMS

- (i) What systems hold the data and from where are each accessible (system accessible and data accessible)?
- (ii) What systems use data and from where are each accessible (system accessible and data accessible)? (Use includes act upon data, such as transfer or process.)

(iii) These questions should provide a good initial list of the factors upon which countries may seek to assert the application of their privacy laws and the basis for their assertion, as well as an understanding of the data and the business.

7. *Legal Analysis*

(a) Which countries may assert a legal basis for the application of their laws based upon the above?

(b) Would countries that may assert such a legal basis be, in so doing, in conflict with the laws of other countries?

(c) Identify all relevant laws.

8. *Risk/Enforcement Analysis*

(a) Which countries that may assert a legal basis have the ability to enforce their laws upon the company? What are the factors, if any, that may influence the enforcement decision?

(b) As to the countries that may enforce their laws on the company, which matter to the business (have the ability to cause financial or reputational harm)? Do they matter equally? Can the company come up with an order of prioritization if trade-offs or competing interests are implicated?

(c) What are the corresponding triggers (impacted data by type and/or system) for each of the potential enforcement actions?

(d) What is the company's current or anticipated ability to design workarounds, i.e. modify, segregate, anonymize, delete, protect, restrict, and otherwise render the data processing compliant?

(e) What are the costs (financial and non-financial) for each proposed design-around? Balanced against the cost of non-compliance?

9. *Arriving at a governance plan*

(a) Organize the information collected in Sections vi-viii in a decision matrix to determine which countries, laws and personal data should be addressed and how to do it. As to each right that involves multiple countries, take the highest standard as to that right and supplement that standard to the extent it does not cover the obligations of other jurisdictions that present risk. Reassess risk based upon substantial compliance with laws of other countries as to each right.

(b) Sections i-v should be developed with the goal of guiding this process.

C. The Hybrid Approach

1. We are presented with two choices, one is global, a one-size-fits-all scenario and two is localized, a country-by-country approach. We argue there is a third option, which we referred to as the Hybrid Approach. The Hybrid Approach is bucketing.

2. What is meant by “bucketing”? Many of geographic regulations borrow or explicitly state they are adhering to an existing regulation. For example, California modeled its privacy regulations after Europe’s GDPR. In fact, there are many countries, states, and provinces that modeled their regulations after GDPR. Yet businesses need to be keenly aware of their marketplaces to determine their buckets, both geographic opportunities and industrial opportunities.

3. Therefore, we leave it up to the WG11 full working group or more likely, the companies themselves to develop these buckets. For the global corporations know their product and necessary constraints and environment that exists in order to be compliant and successful. What we have forged is a framework for which to approach global regulations, not dictate. The buckets are not meant to be evenly distributed but developed to exist based on opportunity and marketplace. Buckets for one global company, most likely will not be the same as another, even if they are competing in the same marketplace.

4. One aspect would be to bucket geographically by similar and shared regulations to reduce the buckets to a manageable number. Another aspect would be to consider industry specific regulations across the geographical locations. We need to be acutely aware of the industry specific regulations that are in effect across geographical areas and should take the same approach to the industry regulations, by bucketing the similar types, as we would do with the geographical regulations.¹

D. “Reasonableness” Approach

1. Drafting team may list regulations and statutes for security and privacy, noting that they require security controls and programs to be “reasonable,” or that there is a risk basis for their design and effectiveness.²

(a) Consider whether to discuss cybersecurity requirements that are part of contracts.³

¹ Appendix B lists regulations based on both geography and industry. This is not exhaustive, but starts to describe the landscape.

² Appendix C lists some regulations that have a reasonable-based approach to privacy or security.

³ See, e.g. False Claims Act news story re cybersecurity.

2. Similarly, other regulations and statutes related to the protection of consumers relative to their information and communications require proactive programs to maintain compliance.⁴

3. The draft team should distinguish between regulatory regimes for which a reasonableness standard would equate with compliance and those which have specific rules not subject to a broad reasonableness definition.

(a) Reasonableness of security controls could authoritatively address security regulations and statutes.

(b) Privacy regulations (HIPAA Privacy Rule, CCPA, etc.) may not provide detailed guidance or prescribe specific practices to be followed. In most cases, an organization's ability to prove that it took reasonable steps will be, at minimum, a factor used to determine fines and penalties.

(i) GDPR is more explicit: "*The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality*"⁵ and describes how privacy controls are to be developed in accordance with the likelihood and impact of risks.⁶

(ii) The drafting team may consider that in some circumstances strict adherence to privacy requirements may create an undue burden for some organizations. Such circumstances may be addressed if a reasonable application of a privacy control can be designed and implemented.

4. The drafting team may wish to provide examples of good practice based on established standards, both domestic and international. Proactive management should be aligned with or driven by standards for managing security and privacy that are developed by professional communities.

(a) *Objectives* for a security program can be stated at a high level, helping organizations plan for the lifecycle of security and privacy threats, regardless of the specific controls they select. Specifically, the drafting team may find it useful to reference the high-level frameworks published by NIST and NIST should be examined and discussed extensively.⁷

⁴ Examples include: Federal Trade Commission Act (15 U.S.C. § 45), Telephone Consumer Protection Act, CAN-SPAM Act, Children's Online Privacy Protection Act, Fair Credit Reporting Act, Electronic Communications Privacy Act, Stored Communications Act, Computer Fraud and Abuse Act, Dodd-Frank Wall Street Reform and Consumer Protection Act (CFPB enablement statute).

⁵ GDPR, Recital 4.

⁶ GDPR, Recitals 76 and 77.

⁷ NIST Cybersecurity Framework v1.1 and NIST Privacy Framework (Draft).

(b) *Controls* that organizations may use to ensure security and privacy should be selected from controls standards. Examples include:

- (i) Those that explicitly address security and privacy
 - (a) NIST Special Publications 800-53 rev 4 and later.
 - (b) AICPA's Trust Criteria, 2017 and later.
- (ii) Those that specifically address security
 - (a) ISO 27002,
 - (b) CIS Controls, and
 - (c) PCI DSS.

(c) *Management processes* that organizations may use to identify requirements, responsibilities, and areas of concern, to develop plans for addressing those items, and to evaluate and improve weaknesses in their environment should be based on known-effective governing principles. The information security community presents standards such as:

- (i) NIST Special Publications 800-37 Rev. 2 and later, and
- (ii) ISO 27001.

(d) *Reasonableness of security controls* and investments can be determined or demonstrated through risk assessments.

(i) Information security risk assessment standards and methods are provided by the information security community. Examples include:

- (a) NIST Special Publications 800-53, and
- (b) ISO 27005.
- (c) RISK IT
- (d) CIS Risk Assessment Methods (CIS RAM)
- (e) Factor Analysis for Information Risk (FAIR)
- (f) Applied Information Economics (AIE)

(ii) Risk assessments are required by standards and regulations to evaluate controls for reasonableness, given the estimated likelihood and impact of threats to the

environment. Because of this, “reasonableness” should be used by organizations as a core standard they should maintain.

(iii) Risk analysis should estimate the likelihood and impact of threats. This is distinct from security assessment methods that evaluate controls based on gaps or maturity.

(e) *Risk treatment plans* should schedule implementation and improvement of identified weaknesses.

(i) Management should track progress on scheduled efforts and investments.

(ii) Prioritization of the plan should be based on risk – at least in part. Organizations may prioritize remediation of their highest risks first, may prioritize projects that reduce risks most efficiently, or by some other risk-related criteria. Organizations may have other compelling bases for prioritization, such as the speed at which they can reduce some risks, compliance with strict standards, and demands from interested parties.

(iii) If risk treatment controls are evaluated using the same analysis that evaluates the risk, then the controls can be compared. This helps organizations determine whether controls are “reasonable” as the Learned Hand Rule implies. This is explained below in the “Definition of “reasonableness” section below.

5. Definition of “reasonableness”

(a) See WG 11 definition (if available).

(b) Provide definition (if WG 11 paper is not yet available).

(i) Risks should be evaluated as described in information security frameworks and regulations, and similarly to multifactor balancing tests in negligence cases.

(a) Risks are evaluated by estimating at least two components; likelihood and impact. These components are similar to ‘liability’ and ‘probability’ used in the Learned Hand Rule.

(c) Risks should consider the likelihood of harm that may come to any interested party, not only to the organization responsible for managing risk.

(i) Risk assessments that drive risk management programs very often fall short by neglecting risk to others in their evaluations and risk acceptance criteria.

(ii) Risks should also be described based upon legal duties imposed by statute or regulation. Risk assessments that overly focus on inward-facing threats and overly objective risk acceptance criteria may fail to adequately measure the organization's practical risk levels. (i.e. we should recognize the limits of "risk calculus", particularly in jury cases where the Learned Hand Rule is largely unused; restated, there are lies, damn lies, and then there are statistics—which include "fuzzy math" that may lie at the heart of quantitative risk analysis methodologies)

(iii) Security controls, and the prioritization of a set of controls (or a plan) in a proactive program should be evaluated using the same criteria that were used to evaluate risk. This helps compare burdens to risks.

(a) Burdens may include; reduction in the utility of the risk, reduction in the benefit that the public or interested parties enjoy from the risk, costs of safeguards related to reductions in profitability or other organizational goals. Burdens may also include additional risks that are created by new safeguards, such as unavailability of information that is excessively difficult to access, or safety issues that result from heavily secured workspaces.

(iv) Impact and likelihood estimates can be described in plain language terms that evaluate whether an impact may be tolerable, intolerable, or catastrophic; or unforeseeable, foreseeable, or expected.

(v) Impact and likelihood estimates can be evaluated using quantitative methods, but could describe in plain language when impacts and likelihoods are tolerable, intolerable, or catastrophic; or unforeseeable, foreseeable, or expected.

6. The draft team may also describe common elements of risk management programs described by security frameworks and required by regulatory regimes, including features such as:

(a) Regular risk assessments to stay apprised of risks to and within the environment.

(i) Usually involving a review of controls (e.g. penetration tests and vulnerability assessments, compliance assessments, etc.)

(b) Regular updates to risk treatment plans and remediation plans.

(c) A process for continuous improvement, whether to eventually achieve compliance, or to reduce the possibility of privacy and security failures even after compliance is achieved.

7. “Burden” applies to the enterprise capability to provide security safeguards, not just burdens at each control.

(a) Where the Learned Hand Rule reminds us to compare the burden of controls to the probability of a liability, organizations often compare each burden to each risk.

(b) However, a proactive program will have one pool of resources to apply to many controls. Therefore, the burden in a proactive program can be defined as the entirety of an enterprise’s mission and objectives being weighed against the entire set of risks that are in the plan to address.

8. The draft team may describe for readers a method for establishing “compliance” with regulations, statutes, or security frameworks.

(a) For requirements that use the standard of “reasonable” controls or controls that present “acceptable risk” organizations may state that they are compliant when all of their controls evaluate as “reasonable.”

(b) For requirements that state that controls are monitored and corrected, organizations may state that they are compliant when they have a risk treatment plan that is based on observed ineffective controls, that the plan is actively and continuously executed, and that vulnerabilities and risks are actively identified.

(c) For requirements that require strict adherence, such as privacy requirements, organizations may state they are compliant when they demonstrate that those controls are in place and operating effectively.

Appendix A – Example Matrix to Combine Multiple Rules

A requirement objective that is found in at least one rule (a security or privacy regulation) is listed first. Because these requirement objectives are commonly found in multiple rules, they can be mapped to specific requirements in each rule (Rules 1 – 3 in this example). An organization can describe the control they have in place to address the requirement objective, then may describe a foreseeable threat that may occur with that control in place. The organization may then estimate the likelihood and impacts of those threats, and can come to a conclusion about the risks priority or acceptability.

Note: The matrix is provided only to illustrate a model for guidance. It does not refer to actual regulations in its Rules columns. As well, the method for recording estimated likelihoods and impacts is not aligned to a specific method, but does imply that risk assessors should have some means for estimating harm in ways that are meaningful to any potentially affected party.

Table 1 - Example Risk Register

Requirement Objective	Rule 1	Rule 2	Rule 3	Control	Threat	Likelihood	Impact	Risk
Asset inventory	5.1.4	§ 122.02	Sec.1.1	All assets on file	Uncontrolled systems may attack network	Expected	All records exposed	Unacceptable
Explicit opt-in at collection	N/A	§ 122.12	Priv.4.1	Detailed approval request on forms	Users may accept without understanding	Uncommon	Few people exercise their rights	Acceptable
Explicit opt-out at collection	N/A	§ 123.13	Priv.4.2	No information gathered without opt-in	N/A	N/A	N/A	N/A
Multifactor authentication	6.2.1	N/A	Sec.2.3	MFA only at applications	Hackers may use stolen network passwords	Expected	Unauthorized control of network	Catastrophic
Vulnerability testing	10.1.3	§ 134.07	Sec.12.2-5	Scans occur weekly. Some vulnerabilities remain	Hackers may exploit vulnerabilities	Uncommon	Unauthorized control of network	Catastrophic
Processing consumer requests	N/A	§ 123.44	Priv.7.1-4	Contacts information and processes in place	Management may not follow through	Unexpected	Few people denied their rights	Unacceptable

Appendix B: Geographical and Industry Regulations

I. GEOGRAPHIC REGULATIONS

A. Europe

1. EU law

- (a) The General Data Protection Regulation (in all EU official languages) –entered into force on 25 May 2018.
- (b) The Data Protection Directive for the law enforcement area (in all EU languages)
- (c) Directive 95/46 for the protection of persons with regard to personal data
- (d) Council framework decision 2008/977 for data protection in the law enforcement area
- (e) ePrivacy Directive 2002/58
- (f) Regulation 45/2001 for the protection of personal data by EU institutions and bodies
- (g) EU-US Privacy Shield – adequacy decision and Annexes in all EU official languages

2. National law

- (a) UK – Data Protection Act (EN)
- (b) Spain – Ley Organica 15/1999 (ES)
- (c) Germany – Bundesdatenschutzgesetz (DE)
- (d) France – Loi n° 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés (FR)
- (e) Romania – Legea 677/2001 (RO)
- (f) Belgium – Loi relative à la protection de la vie privée à l’égard des traitements de données à caractère personnel (FR)
- (g) Bulgaria – Data Protection Law (in EN, provided by the website of the Bulgarian DPA)

(h) Poland – The act of 29 August 1997 on the protection of personal data (in EN, provided by the Polish DPA)

(i) Italy – Personal Data Protection Code (in EN, provided by the Italian DPA)

(j) Greece – Law 2742/1997 and Law 3471/2006 (in EN)

(k) Switzerland (not EU member) - The Swiss Federal Data Protection Act (DPA)

B. United States

1. Federal laws

(a) Driver's Privacy Protection Act of 1994 – 18 U.S. Code 2721 and following

(b) Family Educational Rights and Privacy Act of 1974 (FERPA) – 20 U.S. Code section 1232g

(c) Fair Credit Reporting Act (FCRA) – 15 U.S. Code sections 1681-1681u

(d) Fair Debt Collection Practices Act – 15 U.S. Code sections 1692-1692p

(e) Federal Privacy Act of 1974 – 5 U.S. Code section 552a

(f) Financial Services Modernization Act of 1999, Gramm-Leach-Bliley (GLB), Privacy Rule – 15 U.S. Code sections 6801-6809

(g) Video Privacy Protection Act of 1988 – 18 U.S. Code section 2710

(h) Health Insurance Portability and Accountability Act (HIPAA)

(i) Health Information Technology for Economic and Clinical Health (HITECH)

(j) Electronic Communications Privacy Act 1986 (ECPA); U.S. Code sections 2510-2522, 2701-2711, 3121,1367

(k) Child Online Privacy Protection Act (COPPA)

(l) Cable Communications Privacy Act (CCPA)

(m) Video Privacy Protection Act (VPPA)

2. State laws

- (a) California – Several laws
- (b) Michigan – Internet Privacy Protection Act
- (c) Tennessee S.B. 2005
- (d) Illinois HB1260
- (e) New Mexico HB15

C. Canada

1. Federal laws

- (a) Privacy Act (R.S.C., 1985, c. P-21) (personal data processing by federal government and agencies)
- (b) Personal Information Protection and Electronic Documents Act (PIPEDA- federal private-sector privacy law)

2. Province laws

- (a) Alberta: *Personal Information Protection Act*
- (b) British Columbia: *Personal Information Protection Act*
- (c) Québec: An Act Respecting the Protection of Personal Information in the Private Sector
- (d) Ontario – *Personal Health Information Protection Act*
- (e) New Brunswick – *Personal Health Information Privacy and Access Act*
- (f) Newfoundland and Labrador’s – *Personal Health Information Act*

D. South America

- (a) Argentina – Ley 25.326. Proteccion de los Datos Personales
- (b) Peru – Ley de Proteccion de Datos Personales Ley No 29733
- (c) Brazil – Lei Geral de Protecao de Dados (LGPD)

E. Asia

- (a) Asia-Pacific Economic Cooperation (APEC) Privacy Framework
- (b) Japan – Amended Act of the Protection of Personal Data (EN – unofficial translation)
- (c) Philippines - The Data Privacy Act of 2012

F. Australia

- 1. Commonwealth *Privacy Act 1988* including:
- 2. *Privacy Amendment (Private Sector) Act 2000* and the
- 3. National Privacy Principles (NPPs) & associated Guidelines

G. Africa

- 1. Morocco – Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

II. INDUSTRY REGULATIONS

A. Health

- 1. HIPAA (Health Insurance Portability and Accountability Act) - This act is a two-part bill. Title I: protects the health care of people who are transitioning between jobs or are laid off. Title II: meant to simplify the healthcare process by shifting to electronic data. Also it protects the privacy of individual patients.

- 2. HITECH

B. Finance

- 1. Sarbanes Oxley Act - This act requires companies to maintain financial records for seven years. It was implemented to prevent another Enron scandal.
- 2. Gramm Leach Bliley Act (GLBA) - This act allowed insurance companies, commercial banks, and investment banks to be within the same company. As for security, it mandates that companies secure the private information of clients and customers.
- 3. Payment Card Industry Data Security Standard (PCI-DSS) - A set of 12 regulations designed to reduce fraud and protect customer credit card information.

4. Fair Credit Reporting Act - applies the principles of the Code of Fair Information Practice to credit reporting agencies. The FCRA allows individuals to opt out of unwanted credit offers

C. Federal Government

1. Federal Information Security Management Act of 2002 (FISMA) - This act recognized the information security as matters of national security. Thus, it mandates that all federal agencies develop a method of protecting the information systems.

D. Education

1. Family Educational Rights and Privacy Act (FERPA) - Section 3.1 of the act is concerned with protecting student educational records.

E. Consumer

1. 1970 U.S. Fair Credit Reporting Act
2. 1970 U.S. Racketeer Influenced and Corrupt Organization (RICO) Act
3. 1974 Family Educational Rights and Privacy Act (FERPA)
4. 1974 U.S. Privacy Act
5. 1980 Organization for Economic Cooperation and Development (OECD)
6. 1984 U.S. Medical Computer Crime Act
7. 1984 U.S. Federal Computer Crime Act (strengthened in 1986 and 1994)
8. 1986 U.S. Computer Fraud and Abuse Act (amended in 1986, 1994, 1996 and 2001)
9. 1986 U.S. Electronic Communications Privacy Act (ECPA)
10. 1988 U.S. Video Privacy Protection Act
11. 1990 United Kingdom Computer Misuse Act
12. 1991 U.S. Federal Sentencing Guidelines
13. 1992 OECD Guidelines to Serve as a Total Security Framework
14. 1994 Communications Assistance for Law Enforcement Act

15. 1995 Council Directive on Data Protection for the European Union (EU)
16. 1996 U.S. Economic and Protection of Proprietary Information Act
17. 1996 Health Insurance Portability and Accountability Act (HIPAA)
(requirement added in December 2000)
18. 1998 U.S. Digital Millennium Copyright Act (DMCA)
19. 1999 U.S. Uniform Computer Information Transactions Act (UCITA)
20. 2000 U.S. Congress Electronic Signatures in Global National Commerce
Act ("ESIGN")
21. 2001 U.S. Provide Appropriate Tools Required to Intercept and Obstruct
Terrorism (PATRIOT) Act
22. 2002 Homeland Security Act (HSA)
23. 2002 Federal Information Security Management Act of 2002

Appendix C: Regulations with a Reasonable-Based Approach to Privacy

1. General Data Privacy Regulation (Article 32, paragraphs 1 and 2; Recitals 76 and 77)
2. HIPAA Security Rule (§ 164.308(a)(1)(ii)(A) – (B))
3. HIPAA Privacy rule is distinct from the Security Rule and requires specific adherence. However, some privacy practices within the Privacy Rule such as de-identification still have a risk basis.
4. 23 NYCRR Part 500 (e.g. Section 500.02(b)(1)-(2), Section 500.06(a), Section 500.12(a), Section 500.15(a)).
5. Gramm-Leach-Bliley Act Safeguards Rule
6. California Consumer Privacy Act (1798.150. (a) (1))
7. FISMA (44 USC § 3554(b))
8. 201 CMR 17.00 (201 CMR 17.03(2)(b))
9. FTC actions involving data security and privacy
10. Varied State “data breach notification” statutes that have gradually shifted into more substantive data security regulations.