



2019 Data Privacy Compendium

Marisa A. Trasatti
Sean M. Fox

2019 Data Privacy Compendium

Table of Contents

About the Authors.....	5
Introduction.....	6
U.S. Data Privacy Laws.....	6
1. Alabama.....	6
2. Alaska.....	10
3. Arizona.....	13
4. Arkansas.....	15
5. California.....	17
6. Colorado.....	25
7. Connecticut.....	29
8. Delaware.....	30
9. District of Columbia.....	33
10. Florida.....	35
11. Georgia.....	39
12. Guam.....	41
13. Hawaii.....	43
14. Idaho.....	45
15. Illinois.....	47
16. Indiana.....	50
17. Iowa.....	53
18. Kansas.....	55
19. Kentucky.....	57
20. Louisiana.....	59
21. Maine.....	61
22. Maryland.....	63
23. Massachusetts.....	68
24. Michigan.....	73
25. Minnesota.....	76
26. Mississippi.....	78
27. Missouri.....	79
28. Montana.....	82
29. Nebraska.....	85
30. Nevada.....	87
31. New Hampshire.....	90
32. New Jersey.....	92
33. New Mexico.....	33
34. New York.....	97

35. North Carolina.....	100
36. North Dakota.....	103
37. Ohio.....	105
38. Oklahoma.....	107
39. Oregon.....	110
40. Pennsylvania.....	113
41. Puerto Rico.....	115
42. Rhode Island.....	117
43. South Carolina.....	120
44. South Dakota.....	122
45. Tennessee.....	124
46. Texas.....	126
47. Utah.....	128
48. Vermont.....	130
49. Virgin Islands.....	134
50. Virginia.....	135
51. Washington.....	140
52. West Virginia.....	143
53. Wisconsin.....	145
54. Wyoming.....	147

International Data Privacy Laws.....150

1. Europe.....	150
2. Angola.....	159
3. Argentina.....	161
4. Australia.....	163
5. Austria.....	166
6. Bahrain.....	166
7. Belarus.....	167
8. Belgium.....	169
9. Bermuda.....	169
10. Bosnia	175
11. Herzegovina.....	175
12. Brazil.....	177
13. Bulgaria.....	180
14. Canada.....	180
15. Cape Verde.....	219
16. Chile.....	221
17. China.....	222
18. Costa Rica.....	225
19. Croatia.....	228
20. Cyprus.....	228
21. Czech Republic.....	228
22. Denmark.....	228
23. Estonia.....	229

24. Finland.....	229
25. France.....	229
26. Germany	229
27. Greece.....	229
28. Hong Kong.....	230
29. Hungary.....	231
30. India.....	231
31. Ireland.....	234
32. Israel.....	234
33. Italy.....	236
34. Japan.....	236
35. Latvia.....	238
36. Lithuania.....	238
37. Luxembourg.....	239
38. Malaysia.....	239
39. Mexico.....	242
40. Monaco.....	245
41. Netherlands.....	246
42. New Zealand.....	246
43. Norway.....	249
44. Poland.....	249
45. Portugal.....	250
46. Qatar.....	250
47. Romania.....	252
48. Russia.....	252
49. Singapore.....	256
50. Slovenia.....	258
51. South Africa.....	258
52. South Korea.....	263
53. Spain.....	266
54. Sweden.....	266
55. Switzerland.....	266
56. Taiwan.....	269
57. Thailand.....	271
58. Turkey.....	272
59. UAE-Dubai.....	274
60. Ukraine.....	277
61. United Kingdom.....	280
Conclusion.....	280

About the Authors



Marisa Trasatti is a Partner at Wilson Elser. She focuses her practice primarily on civil litigation, with an emphasis on product liability litigation. She serves as outside General Counsel for Sciton, Inc., a medical and dermatological laser company based in Palo Alto, California. She handles a broad spectrum of matters related to corporate, employment, regulatory, contract and product liability issues in the United States and abroad in connection with her work for Sciton. Marisa also litigates, as local and/or national counsel, toxic tort, general products liability, medical malpractice, and insurance defense cases. Marisa completed her law degree at the University of Maryland School of Law.



Sean Fox is an Associate at Wilson Elser. He handles general liability, toxic tort, and drug and medical device matters for insurers and self-insured entities. Sean completed his law degree at the University of Baltimore School of Law. During law school, he served on the University of Baltimore's Law Review and was a member of the John J. Gibbons Criminal Procedure Moot Court Team. He was awarded University of Baltimore School of Law's Law Faculty Award for Most Outstanding Day Student.

Introduction

Welcome to Wilson Elser LLP's 2019 Data Privacy Compendium. Understanding cybersecurity regulations around the world is critical when collecting and retaining an individual's personal information. Organizations are thus tasked with understanding complex, multi-jurisdictional rules and guidelines or risk severe monetary and criminal penalties. This Compendium provides an overview of the key data privacy laws affecting businesses today.

Changes in data privacy are driven mostly by efforts to keep up with innovation in technology.¹ As technology advances, companies are developing strategic ways to collect user information to achieve certain objectives, such as tracking consumer behavior and compiling consumer databases. New data privacy laws serve the purpose of regulating the collection activities by giving internet users more control over information that is collected and shared.²

The 2019 Data Privacy Compendium should act as a primer to businesses as they consider this complex and evolving area of compliance. Depending upon the nature of your client's product, you will also want to consult the applicable regulatory body including FDA, FTC, etc. We hope that you find this compendium a helpful go-to resource.

I. United States

In the wake of global data breaches and tough new data privacy requirements adopted by the European Union and California, the Federal Government is competing to establish a federal data privacy framework to align the interests of its citizens and organizations. According to White House spokeswoman Lindsay Walters, the goal is a policy "that is the appropriate balance between privacy and prosperity."³ For now, however, businesses seeking to enact compliance protocols must obey data privacy rules and regulations adopted by individual states.

1. Alabama

Ala. Code § 8-38-12 (1975)

Protection of Personal Information

Covered entities⁴ and their third-party⁵ agents must implement and maintain reasonable security

¹ Adam Satariano, The New York Times, What the G.D.P.R., Europe's Tough New Data Law, Means for You (2018), <https://www.nytimes.com/2018/05/06/technology/gdpr-european-privacy-law.html>.

² *Id.*

³ David Meyer, Fortune, In the Wake of GDPR, Will the U.S. Embrace Data Privacy? (2018), <http://fortune.com/2018/11/29/federal-data-privacy-law/>.

⁴ "Covered entity" means a person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information.

⁵ "Third-party agent" is defined as "an entity that has been contracted to maintain, store, process, or is otherwise

measures to protect sensitive personally identifying information against a breach of security, which include:

- Designation of an employee(s) to coordinate the covered entity's security measures to protect against a breach of security;
- Identification of internal and external risks of a breach of security;
- Adoption of appropriate information safeguards to address identified risks of a breach of security and assess the effectiveness of such safeguards;
- Retention of service providers that are contractually required to maintain appropriate safeguards for sensitive personally identifying information;
- Evaluation and adjustment of security measures to account for changes in circumstances affecting the security of sensitive personally identifying information; and
- Keeping the management of the covered entity, including its board of directors, if any, appropriately informed of the overall status of its security measures.

The law also contains a data disposal provision that requires covered entities and third-party agents to shred, erase or otherwise modify sensitive personally identifying information contained in records when the records are no longer to be retained pursuant to applicable law, regulations or business needs.

What information is protected?

“Sensitive personally identifying information” means the following:

- An Alabama resident's first name or first initial and last name in combination with one or more of the following:
 - A non-truncated social security number or tax identification number;
 - A non-truncated driver's license number, state-issued identification card, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual;
 - A financial account number, including a bank account number, credit card number, or debit card number, in combination with any security code access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account;

permitted to access sensitive personally identifying information in connection with providing services to a covered entity.”

- Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;
- An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual;
- A user name or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information.

Sensitive personally identifying information **is not** information that is truncated, encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable, including encryption of the data, document, or device containing the sensitive personally identifying information, **unless** the covered entity **knows or has reason to know** that the encryption key or security credential that could render the personally identifying information readable or useable has been breached together with the information.

Notification of Breach

If a covered entity determines that a breach of security⁶ has or may have occurred in relation to sensitive personally identifying information that is accessed, acquired, maintained, stored, utilized, or communicated by, or on behalf of, the covered entity, the covered entity shall conduct a **good faith and prompt investigation**.

If a covered entity determines that sensitive personally identifying information **has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates, shall give notice** of the breach to each individual.

Third Party: In the event a third-party agent has experienced a breach of security in the system maintained by the agent, the agent shall notify the covered entity **as expeditiously as possible and without unreasonable delay, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred**. A third-party agent, in cooperation with a covered entity, shall provide information in the possession of the third-party agent so that the covered entity can comply with its notice requirements. A covered entity may enter into a contractual agreement with a third-party agent whereby the third-party agent agrees to handle notifications required under this act.

Notice to individuals shall be made **as expeditiously as possible without unreasonable delay**,

⁶ "Breach of security" means the unauthorized acquisition of data in electronic form containing sensitive personally identifying information. Acquisition occurring over a period of time committed by the same entity constitutes one breach.

taking into account the time necessary to allow the covered entity to conduct the required investigation. The covered entity shall provide notice **within 45 days** of the covered entity's receipt of notice from a third-party agent that a breach has occurred or upon the covered entity's determination that a breach has occurred and is **reasonably likely to cause substantial harm to the individuals** to whom the information relates.

If a federal or state law enforcement agency determines that notice to individuals required under this section would interfere with a criminal investigation or national security, the notice shall be delayed upon the receipt of written request of the law enforcement agency for a period that the law enforcement agency determines is necessary.

If a covered entity determines that **notice is not required**, the entity shall document the determination in writing and maintain records concerning the determination for no less than **five years**.

Requirements for Notification

The notice shall include, at a minimum, all of the following:

- The date, estimated date, or estimated date range of the breach;
- A description of the sensitive personally identifying information that was acquired by an unauthorized person as part of the breach;
- A general description of the actions taken by a covered entity to restore the security and confidentiality of the personal information involved in the breach;
- A general description of steps an affected individual can take to protect himself or herself from identity theft;
- Information that the individual can use to contact the covered entity to inquire about the breach.

Notice to the individual in shall be given in **writing**, sent to the mailing address of the individual in the records of the covered entity, **or by email** notice sent to the email address of the individual in the records of the covered entity. Substitute notice may be provided in lieu of direct notice, if direct notice is not feasible due to any of the following:

- Excessive cost. The term includes either of the following:
 - Excessive cost to the covered entity relative to the resources of the covered entity;
 - The cost to the covered entity exceeds five hundred thousand dollars;
- Lack of sufficient contact information for the individual required to be notified;
- The affected individuals exceed **100,000** persons.

Substitute notice shall include both of the following:

- A conspicuous notice on the internet website of the covered entity, if the covered entity maintains a website, for a period of 30 days;
- Notice in print and in broadcast media, including major media in urban and rural areas where the affected individuals reside.

If the number of individuals a covered entity is required to notify exceeds **1,000**, the entity shall provide written notice of the breach to the **attorney general** as expeditiously as possible and without unreasonable delay, **but no later than 45 days**, subject to the needs of law enforcement, after the covered entity either receives notice of a breach from a third party agent or determines that a breach has occurred. Written notice to the attorney general shall include:

- A synopsis of the events surrounding the breach at the time that notice is provided;
- The approximate number of individuals in the state who were affected by the breach;
- Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions on how to use the services;
- The name, address, telephone number, and email address of the employee or agent of the covered entity from whom additional information may be obtained about the breach.

If a covered entity discovers circumstances requiring notice of more than **1,000** individuals at a single time, the entity shall also notify, **without unreasonable delay**, all consumer reporting agencies of the timing, distribution, and content of the notices.

Penalty

The statute does not create a private right of action.

Violations of the notification provisions are unlawful trade practices under the Alabama Deceptive Trade Act, Chapter 19, Title 8. The Attorney General has exclusive authority to bring an action for civil penalties under the statute. Covered entities may be liable for a civil penalty of **not more than \$5,000 per day** for each consecutive day the covered entity fails to notify affected individuals. The Attorney General may also bring an action in a representative capacity on behalf of any named individuals, in which recovery is limited to actual damages suffered by the individuals plus reasonable attorneys' fees and costs.

The Alabama law imposed civil penalties up to \$500,000 per breach for any entity that knowingly violates or fails to comply with the notification provisions.

2. Alaska

Alaska Stat. § 45.48.010 (2009)

What information is protected?

The law defines “personal information” means information in any form on an individual that is not encrypted or redacted, or is encrypted and the encryption key has been accessed or acquired, and that consists of a combination of:

- An individual’s name, which may be a combination of first name or first initial and last name; and one or more of the following information elements:
 - Social security number;
 - Driver’s license number;
 - Account number, credit card number, or debit card number;
 - If an account can only be accessed with a personal code, an account number, credit card number, or debit card number and the personal code (security code, access code, a personal identification number, or a password);
 - Passwords, personal identification numbers, or other access codes for financial accounts.

Notification of Breach

If a covered person⁷ owns or licenses personal information in any form that includes personal information on a state resident, and a breach of the security⁸ of the information system that contains personal information occurs, the covered person shall, **after discovering or being notified of the breach**, disclose the breach to each state resident whose personal information was subject to the breach.

An information collector⁹ shall make disclosure in the **most expeditious time possible without unreasonable delay**.

Notification is **not required** if after an appropriate investigation and after written notification to the attorney general of this state, the covered person determines that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach. The determination shall be documented in writing, and the documentation shall be maintained for five years.

⁷ A “covered person” includes: (A) a person doing business; (B) governmental agency; or (C) person with more than 10 employees.

⁸ “Breach of security” means unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information by the information collector; in this paragraph, “acquisition includes acquisition by: (A) photocopying, **facsimile, or other paper-based method**; (B) **a device, including a computer, that can read, write, or store information that is represented in numerical form**; or (C) a method not identified by (A) or (B).

⁹ An “information collector” means a covered person who owns or licenses personal information in any form if the personal information includes personal information from a state resident.

If a breach of the security of the information system containing personal information of a state resident that is maintained by an information recipient occurs, the information recipient is not required to comply with AS 45.48.010 - 45.48.030. However, immediately after the information recipient discovers the breach, the information recipient shall notify the information distributor who owns the personal information or who licensed the use of the personal information to the information recipient about the breach and cooperate with the information distributor as necessary to allow the information distributor to comply with this statute. In this subsection, "cooperate" means sharing with the information distributor information relevant to the breach, except for confidential business information or trade secrets.

Requirements for Notification

Notification shall include **at least** the following:

- Written document sent to the most recent address the information collector has for the state resident;
- By electronic means if the information collector's primary method of communication with the state resident is by electronic means; or
- The information collector demonstrates that the cost of providing notice would exceed \$150,000, that the affected class of state residents to be notified exceeds 300,000, or that the information collector does not have sufficient contact information to provide notice, by
 - Electronic mail if the information collector has an electronic mail address for the state resident;
 - Conspicuously posting the disclosure on the internet website of the information collector if the information collector maintains an internet website; and
 - Providing a notice to a major statewide media.

If an information collector is required to **notify more than 1,000 state residents** of a breach, the information collector shall **also** notify without unreasonable delay **all** consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis and provide the agencies with the timing, distribution, and content of the notices to state residents.

Notification may be delayed if a law enforcement agency advises the person that the notifications will impede a criminal investigation.

Penalty

If an information collector violates Alaska Stat. §§ 45.48.010 *et seq.* with regard to the personal information of a state resident, the violation is an unfair or deceptive act or practice under Alaska Stat. §§ 45.50.71–45.50.561. However,

- The information collector is not subject to the civil penalties imposed under Alaska Stat. § 45.50.551 but is still liable to the state for a civil penalty of up to \$500 for each state resident who was not notified under Alaska Stat. §§ 45.48.010–45.48.090, except that the total civil penalty may not exceed \$50,000; and
- Damages that may be awarded against the information collector under:
 - Alaska Stat. § 45.50.531 (class action for unfair or deceptive act or practice) are limited to actual economic damages that do not exceed \$500; and
 - Alaska Stat. § 45.50.537 (attorney fees, costs, and damages for unfair or deceptive act or practice) are limited to actual economic damages.

3. Arizona

Ariz. Rev. Stat. § 44-7501 (2006), as amended (2007, 2016, 2018)

Effective August 1, 2018, the House Bill 2154 recently signed by the Arizona governor will expand the current Arizona data breach notification law.

What information is protected?

The new law defines “personal information” as:

- An individual’s first name or first initial and law name in combination with one or more specified data elements;
 - A “specified data element” means: an individual’s Social Security number, driver’s license number, financial account or credit card number, health insurance identification number, information about an individual’s medical or mental health treatment or diagnosis by a health care professional, passport number, tax payer identification number, or unique biometric data.
- An individual’s user name or e-mail address, in combination with a password or security question and answer, that allows access to an online account.

Notification of Breach

If a person¹⁰ that conducts business in Arizona and that owns, maintains or licenses **unencrypted and unredacted** computerized personal information **becomes aware** of a security incident, the person shall conduct an investigation to promptly determine whether there has been a security

¹⁰ A “person” means a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government or governmental subdivision or agency or any other legal or commercial entity.

system breach.

If the investigation results in a determination that there has been a security system breach¹¹, the person that owns or licenses the computerized data, **within forty-five days after the determination** shall:

- Notify the individuals affected (subject to the notification requirements below); and
- If the breach requires notification of more than **one thousand individuals**, notify both:
 - The three largest nationwide consumer reporting agencies; and
 - The attorney general, in writing, in a form prescribed by rule or order of the attorney general or by providing the attorney general with a copy of the notification provided above.

Notification may be delayed if a law enforcement agency advises the person that the notifications will impede a criminal investigation.

However, **a person is not required to make the notification required above if the person, an independent third-party forensic auditor or law enforcement agency determines after a reasonable investigation that a security system breach has not resulted in or not reasonably likely to result in substantial economic loss to affected individuals.**

A person who maintains unencrypted and unredacted computerized personal information that the person does not own shall notify and cooperate with the owner or the licensee of the personal information, including sharing information relevant to the breach with the owner or licensee. The person who owns or licenses the computerized data shall provide notice to the individual pursuant to this section. The person who maintains the data under an agreement with the owner or licensee is not required to provide notifications to the individual unless the agreement stipulates otherwise.

Requirements for Notification

Notification shall include **at least** the following:

- The approximate date of the breach;
- A brief description of the personal information included in the breach;
- The toll-free numbers and address for the three largest nationwide consumer reporting agencies;

¹¹ “Breach” or “security system breach” means an unauthorized acquisition of an unauthorized access that **materially compromises the security or confidentiality of unencrypted and unredacted computerized personal information** maintained as part of a database of personal information regarding multiple individuals.

- The toll-free number, address and website address for the federal trade commission or any federal agency that assists consumers with identity theft matters.

The notification shall be provided by one of the following methods:

- Written notice;
- An email notice if the person has email address for the individuals who are subject to the notice;
- Telephone notice, if telephonic contact is made directly with the affected individuals and is not through a prerecorded message.
- Substitute notice if the person can demonstrate that notice pursuant to the aforementioned methods would exceed fifty thousand dollars, that the affected class of subject individuals to be notified exceeds one hundred thousand individuals, or that the person does not have sufficient contact information. Substitute notice consists of:
 - A written letter to the attorney general that demonstrates the facts necessary for substitute notice;
 - Conspicuous posting of the notice for at least forty-five days on the website of the person if the person maintains one.

Penalty

The attorney general may impose a civil penalty for a **knowing and willful** violation of this article not to exceed the lesser of ten thousand dollars per affected individual or the total amount of economic loss sustained by affected individuals, but the **maximum** civil penalty from a breach or series of related breaches may not exceed **five hundred thousand dollars**.

4. Arkansas

Ark. Code Ann. §§ 4–110–101 (2005) (“Personal Information Protection Act”)

What information is protected?

“Personal information” means:

- an individual’s first name or first initial and his or her last name in combination with any of the following data elements when either the name or the data element is not encrypted or redacted:
 - Social security number;
 - Driver’s license number or Arkansas identification card number;

- Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; and
- Medical information.

Protection of Personal Information

A person or business shall take all **reasonable steps** to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

A person or business that acquires, owns, or licenses personal information about an Arkansas resident **shall implement and maintain reasonable security procedures and practices** appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

Notification of Breach

Any person or business that acquires, owns, or licenses computerized data that includes personal information shall disclose any breach of the security of the system **following discovery or notification of the breach of the security of the system**¹² to any resident of Arkansas whose **unencrypted** personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The disclosure shall be made in the **most expedient time and manner possible without unreasonable delay**.

Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Notification may be delayed if a law enforcement agency advises the person that the notifications will impede a criminal investigation.

However, **Notification under this section is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.**

Requirements for Notification

Ark. Code Ann. §§ 4-110-101 –108 **does not** have specific content requirements.

¹² "Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business.

The notification shall be provided by one of the following methods:

- Written notice;
- Electronic mail notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001, as it existed on January 1, 2005; or
- Substitute notice if the person or business demonstrates that:
 - The cost would exceed **two hundred fifty thousand dollars**;
 - The affected class of persons to be notified exceeds **five hundred thousand**; or
 - The person or business does not have sufficient contact information.
- Substitute notice consists of
 - Electronic mail notice when the person or business has an electronic mail address for the subject persons;
 - Conspicuous posting of the notice on the website of the person or business if the person or business maintains a website; and
 - Notification by statewide media.

Penalty

Any violation of this statute is punishable by action of the Attorney General.

Any person who knowingly and willfully commits an unlawful practice under [the Personal Information Protection Act] shall be guilty of a Class A misdemeanor.

The Attorney General has the authority, acting through the Consumer Counsel, to file an action for civil enforcement of the provisions of this chapter, including, but not limited to, the seeking of restitution and the seeking of an injunction prohibiting any person from engaging in any deceptive or unlawful practice prohibited by this statute.

5. California

1. Cal. Civ. Code §1798.82, as amended (2016), 1798.84

Protection of Personal Information

A business that owns, licenses, or maintains personal information about a California resident **shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.**

A business shall take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

Third Party: A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party that is not subject to subdivision (b) shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

What information is protected?

“Personal information” means either of the following:

- An individual’s first name or first initial and last name in combination with any one or more of the following elements, when either the name or the data elements are **not encrypted:**
 - Social security number;
 - Driver’s license number or California identification number;
 - Account number or credit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
 - Medical information;
 - Information or data collected through the use or operation of an automated license plate recognition system.
- A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

Notification of Breach

A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of

the system¹³ **following discovery** or notification of the breach in the security of the data to a resident of California **(1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable.**

The disclosure shall be made in the **most expeditious time** possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

A person or business that maintains computerized data that includes personal information that the person or business **does not own** shall notify the owner or licensee of the information of the breach of the security of the data immediately **following discovery**, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The notification required by this section **may be delayed if a law enforcement agency** determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

Requirements for Notification

General Breach Notification Statute

The security breach notification to California residents must be in written form, using plain language in no smaller than 10-point type. The notification shall be titled “Notice of Data Breach,” and use the following clearly and conspicuously displayed headings:

- “What Happened;”
- “What Information was Involved;”
- “What We Are Doing;”

¹³ “Breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

- “What You Can Do;” and
- “For More Information.”

The breach notification **must** include at least the following elements:

- The name and contact information of the reporting person or business subject to this section.
- A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
- If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.
- Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
- A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.
- If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

Breach involving Username or Email Address:

In the case of a breach of the security system of personal information specifically involving a username or email address, in combination with a password or security question and answer that would permit access to an online account *and no other personal information*, breach notification to California residents may be in electronic or other form that directs the person whose personal information has been breached to promptly change his or her password and security question or answer, or to take other steps appropriate to protect the online account and all other online accounts

where the person uses the same username or email address and password or security question or answer.

In the case of a breach of the security system involving personal information consisting of login credentials of an email account furnished by an entity, the entity shall not provide notice by that email address but by providing notice by another method or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an IP address or online location from which the entity knows the resident customarily accesses the account.

A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General.

<https://oag.ca.gov/privacy/databreach/report-a-breach>.

Penalty

Any customer injured by a violation of this title may institute a civil action to recover damages. Any business that violates, proposes to violate, or has violated this title may be enjoined.

2. Consumer Privacy Act of 2018 (“CCPA”) (2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (WEST)): Beginning January 1, 2020

a. Overview

When does it go into effect?

The new law will go into effect on January 1, 2020.

What does the law say?

The California Consumer Privacy Act of 2018 grants a right of privacy for the collection and sale of personal information. In short, the new law gives consumers the right to ask businesses for the types and categories of personal information being collected. It also requires businesses to disclose the purpose for collecting or selling the information as well as the identity of the third-party organizations receiving the data. Consumers can also request data be deleted and initiate civil action if they believe that an organization has failed to protect their personal data.

Predicted Changes for CCPA

The new law was backed by the tech industry as they preferred to agree to these new standards than see a more powerful proposal put to voters on the ballot (which was the initial plan). This new law was rushed through a bipartisan vote to avoid complexities that would arise if the proposal was placed on a ballot instead, and therefore, many predict that this law will continue to evolve prior to January 1, 2020.

CCPA Compared to GDPR

The Privacy Act is not as intensive as the European Union's GDPR, in that it does not require deliberate opt-in consent for collection of data; however, the Privacy Act does mirror GDPR's theme of an individual's right to control his/her personal information. There are a few important differences that make the California law weaker than GDPR. GDPR gives consumers the right to ask companies to stop collecting information, while the California law gives people the option to ask companies to delete information or stop selling it- but the California law does not prevent companies from collecting information in the first place. Additionally, fines under the CCPA aren't nearly stiff as fines imposed under GDPR.

Personal information under the Act does not include any information that is publicly available. The state law, which goes into effect in 2020, requires more transparency for third parties that handle data. It affects any company that uses application programming interfaces, software development kits and other open development tools to rebuild e-commerce interfaces or digital payment gateways.

The main components of California's new Privacy Act are as follows:

- Consumers have a right to request a business to disclose the categories and specific pieces of personal information that it collects about the consumer, the categories of sources from which the information is collected, the business purposes for collection or selling the information, and the categories of third parties from which the information is shared.
- A business must make disclosures about the information collected and purposes for which it is used. If the Business wishes to collect additional categories of data, the Business should provide the Consumer additional notice.
- Consumers can request deletion of personal information and businesses must comply.
- Consumers have the right to request from Businesses the categories of information that it collects and the identity of third parties in which the data is sold. The Consumer can then request to opt out of the sale of his/her personal information, meaning the business could not sell that person's information. The Business in turn cannot discriminate against that consumer by charging the consumer a higher amount of providing a different quality of goods or services unless the difference is reasonably related to the value of that data.
- Businesses can offer financial incentives for collection of personal information.
- Businesses are prohibited from selling information of persons under the age of 16, without authorization.

Below is a more thorough explanation of the principles and requirements set forth in the Privacy Act.

b. A Consumer's Right to Request Disclosure of the Categories of Personal Information that the Business Collects

A consumer has the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected. The business will only have to provide this level of information *upon receipt of a verifiable consumer request*.

Types of Requests may include:

- Categories of information collected about that consumer;
- Categories of sources of information;
- The purpose for collection/selling;
- Categories of third parties with whom businesses share personal information;
- Specific information a business maintains of that specific consumer.

Verifiable Written Request Defined: A verifiable written request means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer if the business cannot verify that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

Receipt of a Verifiable Written Request: If a company receives a request, it must promptly disclose and deliver, free of charge, the personal information requested. Delivery can be done electronically, if possible, or by regular mail.

Multiple or Unreasonable Requests from the same person: The Act insulates businesses from dealing with repeated, excessive requests. A company is not required to provide personal information to a consumer more than twice in a 12-month period. If the request is manifestly excessive, a business can charge a reasonable fee, taking into account administrative costs of providing the information.

Collection of Additional Categories of Personal Information: If a business would like to begin collecting additional categories, it must first provide the customer notice. Unlike EU's GDPR, there is no consent or opt-in requirement, this is simply a notification requirement.

No Requirement for Businesses to Retain Information: There is no requirement for a business to retain personal information for a single transaction if the information is not sold, or retained by the business or to reidentify/link the information that is not maintained in a manner that would be considered personal information.

c. Right to Request Deletion

A business that collects personal information shall disclose the consumer's right to request deletion. If a company receives a request for deletion, it must delete any personal information and direct service providers to also delete that information.

Instances when businesses do not have to delete even after a request:

- Business needs the personal information to complete a transaction, provide a good/service requested by the consumer within the context of the ongoing relationship between customer/business.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
- Debug to identify and repair errors that impair existing intended functionality.
- Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.
- Comply with state laws on privacy.
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.
- To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.
- Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.
- Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

d. Selling Consumers' Personal Information

Consumers have the right to request that a company disclose certain things prior to selling their personal information:

- Categories of personal information that the business collected about the consumer;
- Categories of personal information sold and to whom it was sold;

- Categories of personal information that the business disclosed for business purposes.

Consumers can direct businesses not to sell their personal information. This is referred to as the right to “opt out.” Businesses should notify consumers in advance of selling their information to third parties.

Minors: If a business has received direction from a consumer not to sell the consumer’s personal information or in the case of a minor’s information, has not received consent to sell the minor’s information, then selling information is prohibited.

Businesses cannot thereafter discriminate against a Consumer because the consumer chose to opt-out of having his/her information sold. However, businesses can offer financial incentives for the collection of personal information, sale of personal information, or deletion of personal information. A company can offer a better price to consumers who do not opt out of having their information sold if that price difference is directly related to the value provided by the personal information.

e. What Methods A Company Must Offer for Consumers to Submit Requests

A company must provide two or more methods for submitting requests for information. Options include a toll free number or a company’s website.

Delivering the Information: A company has 45 days to deliver requested information for verifiable requests. This must be free of charge and information must cover the preceding 12 month period. When reasonably necessary, this 45 day period can be extended an additional 45 days, but a company will need to provide notice of the delay.

If a company plans to sell consumer’s information: Must provide a clear, and conspicuous link on the business’ internet homepage titled “Do Not Sell My Personal Information” and include a description of the consumer’s rights in the online privacy policy. Requests to opt-out must be honored for 12 months before requesting to sell their information again.

f. Allowing Unauthorized Access of Information

The Consumer Privacy Act actually allows any consumer whose personal data is exposed to sue the breached entity for damages ranging from \$100-\$750 or more per exposed record. Further, once you add in all other breach-related costs- IT response, forensics and recovery, legal, notifications, this could push a breach into the realm of an existential threat.

6. Colorado

Colo. Rev. Stat. Ann. § 6-1-716 (2006), as amended (2018)

Protection of Personal Information

Each covered entity¹⁴ in the state that maintains paper or electronic documents during the course of business that contain personal identifying information **shall develop a written policy for the destruction or proper disposal** of those paper and electronic documents containing personal identifying information.

Security Procedures: To protect personal identifying information from unauthorized access, use, modification, disclosure, or destruction, a covered entity that maintains, owns, or licenses personal identifying information of an individual residing in the state **shall implement and maintain reasonable security procedures and practices** that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations.

Third Parties: Unless providing its own security protection, the covered entity shall require that a third-party service provider implement and maintain reasonable security procedures and practices that are:

- Appropriate to the nature of the personal identifying information disclosed; and
- Reasonably designed to help protect the personal identifying information from unauthorized access, use, modification, disclosure, or destruction.

What information is protected?

“Personal information” means either of the following:

- A Colorado resident’s first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are **not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable:**
 - Social security number;
 - Student, military, or passport identification number;
 - Driver’s license number or identification card number;
 - Medical information;¹⁵
 - Health insurance identification number; or
 - Biometric data;¹⁶

¹⁴ “Covered entity” means an individual, corporation, business trust, estate, trust, partnership, unincorporated association or commercial entity that maintains, owns or licenses computerized data that includes personal information about a resident of Colorado.

¹⁵ “Medical Information” means any information about a consumer’s medical or mental health treatment or diagnosis by a healthcare professional.

¹⁶ “Biometric Data” means unique biometric data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when he or she accesses an online account.

- A Colorado resident's username or email address, in combination with a password or security questions and answers, that would permit access to an online account; or
- A Colorado resident's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.

Notification of Breach

A covered entity that maintains, owns, or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware that a security breach¹⁷ may have occurred, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused.

The covered entity shall give notice to the affected Colorado residents **unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur.**

Notice must be made in the **most expedient time possible and without unreasonable delay,** but not later than **thirty days after the date of determination that a security breach occurred**¹⁸, consistent with the legitimate needs of law enforcement.

A third-party service provider that is used by a covered entity to maintain computerized data that includes personal information shall give notice to and cooperate with the covered entity in the event of a security breach. Such notice to the covered entity shall be made in the most expedient time possible and without unreasonable delay following discovery of a security breach, if misuse of personal information about a Colorado resident occurred or is likely to occur. Cooperation includes sharing with the covered entity information relevant to the security breach, except that such cooperation does not require the disclosure of confidential business information or trade secrets.

Notice may be delayed if the notice will impede a criminal investigation and the law enforcement agency has notified the entity that conducts business in Colorado not to send notice. Notice must be made **no later than 30 days** after the law enforcement agency has notified the entity that it is **appropriate** to send the required notice.

Requirements for Notification

In the case of a breach of personal information, notice is required to include, but need not be

¹⁷ "Security breach" means the unauthorized acquisition of **unencrypted** computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity. Good faith acquisition of personal information by an employee or agent of a covered entity for the covered entity's business purposes is not a security breach if the personal information is not used for a purpose unrelated to the lawful operation of the business or is not subject to further unauthorized disclosure.

¹⁸ "Determination that a Security Breach Occurred" means the point in time at which there is sufficient evidence to conclude that a security breach has taken place.

limited to, the following:

- The date, estimated date, or estimated date range of the security breach;
- A description of the personal information that was acquired or reasonably believed to have been acquired as part of the security breach;
- Information that the resident can use to contact the covered entity to inquire about the security breach;
- The toll-free numbers, addresses, and websites for consumer reporting agencies;
- The toll-free number, address, and website for the federal trade commission; and
- A statement that the resident can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

In addition, **for breaches involving usernames/email addresses and password/security questions and answers (login credentials)**, the entity must also direct the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect said person's online accounts that use the same username or email address and password or security question or answer. If the login credentials of an email account furnished by the covered entity are impacted, the covered entity shall not provide notice to that email address, but may provide notice through another method, including conspicuous notice to the resident online when the resident is connected to the online account from an internet protocol address or online location from which the covered entity knows the resident customarily accesses the account.

If a covered entity is required to **notify more than one thousand Colorado residents** of a security breach pursuant to this statute, they **must also notify all consumer reporting agencies** that compile and maintain files on consumers on a nationwide basis.

A covered entity shall provide notice to the Colorado Attorney General not later than **30 days** after the date of determination that a security breach occurred, for breaches reasonably believed to have **affected 500 or more Colorado residents**.

Penalty

The attorney general may bring an action in law or equity to address violations of this section and for other relief that may be appropriate to ensure compliance with this section or to recover direct economic damages resulting from a violation, or both.

7. Connecticut

Conn. Gen. Stat. § 36a-701b (2005); as amended (2012, 2015, 2018)

What information is protected?

“Personal information” means either of the following:

- An individual’s first name or first initial and last name in combination with any one, or more, of the following data:
 - Social Security number;
 - Driver’s license number;
 - Credit or debit card number;
 - Financial account number in combination with any required security code, access code or password that would permit access to such financial account.

Notification of Breach

Any person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information, shall provide notice of any breach of security **following the discovery of the breach¹⁹** to any resident of this state whose personal information was breached or is reasonably believed to have been breached. Such notice shall be made **without unreasonable delay but not later than ninety days after the discovery of such breach**, unless a shorter time is required under federal law.

Such notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person **reasonably determines that the breach will not likely result in harm** to the individuals whose personal information has been acquired and accessed.

Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following its discovery, if the personal information was, or is reasonably believed to have been accessed by an unauthorized person.

Requirements for Notification

Notice to a Connecticut resident may be provided by one of the following methods:

- Written notice;
- Telephone notice;

¹⁹ “Breach of security” means unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data, containing personal information when access to the personal information **has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.**

- Electronic notice, provided such notice is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001;
- Substitute notice, provided such person demonstrates that the cost of providing notice under this section would exceed **two hundred fifty thousand dollars**, that the affected class of subject persons to be notified exceeds **five hundred thousand** persons, or that the person doesn't have sufficient contact information. Substitute notice shall consist of the following:
 - Electronic mail notice when the person has an electronic mail address for the affected persons;
 - Conspicuous posting of the notice on the web site of the person if the person maintains one; and
 - Notification to major state-wide media, including newspapers, radio and television.

The person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information, shall, not later than the time when notice is provided to the resident, **also provide notice of the breach of security to the Attorney General.**

Identity theft prevention services must be provided at no cost, for a period of at least 24 months, to residents whose personal information was breached or is reasonably believed to have been breached from computerized data owned by a Connecticut business.

Penalty

Failure to comply with the requirements of this section shall constitute an unfair trade practice for purposes of section 42-110b and shall be enforced by the Attorney General.

8. Delaware

Del. Code Ann. tit. 6, §§ 12B-100 (2005), as amended (2017)

Protection of Personal Information

Any person ²⁰who conducts business in this State and owns, licenses, or maintains personal information **shall implement and maintain reasonable procedures and practices** to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business.

²⁰ "Person" means an individual; corporation; business trust; estate trust; partnership; limited liability company; association; joint venture; government; governmental subdivision, agency, or instrumentality; public corporation; or any other legal or commercial entity.

What information is protected?

“Personal information” means either of the following:

- A Delaware resident’s first name or first initial and last name in combination with any one or more of the following data elements that relate to that individual:
 - Social Security number;
 - Driver’s license number or state or federal identification card number;
 - Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to a resident’s financial account;
 - Passport number;
 - A username or email address, in combination with a password or security question and answer that would permit access to an online account;
 - Medical history, medical treatment by a healthcare professional, diagnosis of mental or physical condition by a healthcare professional, or deoxyribonucleic acid profile;
 - Health insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person;
 - Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes;
 - An individual taxpayer identification number.

Notification of Breach

Any person who conducts business in this State and who owns or licenses computerized data that includes personal information shall provide notice of any breach of security²¹ **following**

²¹ “Breach of security” means:

- a. The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. Good faith acquisition of personal information by an employee or agent of any person for the purposes of such person is not a breach of security, provided that the personal information is not used for an unauthorized purpose or subject to further unauthorized disclosure.
- b. **The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information is not a breach of security to the extent**

determination of the breach of security²² to any resident of this State whose personal information was breached or is reasonably believed to have been breached, **unless, after an appropriate investigation, the person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached.**

Notice required must be made **without substantial delay but not later than 60 days after determination of the breach of security,** except in the following situations:

- A shorter time is required under federal law;
- A law enforcement agency determines that the notice will impede a criminal investigation. Any such notice must be made after the law enforcement agency determines that notice will not compromise the criminal investigation;
- The covered person cannot through reasonable diligence identify within 60 days certain Delaware residents whose personal information was breached. Such person must provide notice as soon as practicable after the determination that the breach of security included the personal information of such residents.

A person that maintains computerized data that includes personal information that the person does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of security immediately following determination of the breach of security. For purposes of this subsection, “cooperation” includes sharing with the owner or licensee information relevant to the breach.

Requirements for Notification

Del. Code Ann. tit. 6, § 12B-100 *et seq.* **does not** have specific content requirements. If the affected number of Delaware residents to be notified **exceeds 500 residents,** the person required to provide notice shall, not later than the time when notice is provided to the resident, also **provide notice of the breach of security to the Attorney General.**

If the breach of security **includes a Social Security number,** the person shall offer to each resident, whose personal information, including Social Security number, was breached or is reasonably believed to have been breached, **credit monitoring services at no cost** to such resident for a period of **1 year.** Such person shall provide all information necessary for such resident to

that personal information contained therein is encrypted, unless such unauthorized acquisition includes, or is reasonably believed to include, the encryption key and the person that owns or licenses the encrypted information has a reasonable belief that the encryption key could render that personal information readable or useable.

²² “Determination of the breach of security” means the point in time at which a person who owns, licenses or maintains computerized data has sufficient evidence to conclude that a breach of security of such computerized data has taken place.

enroll in such services and shall include information on how such resident can place a credit freeze on such resident's credit file. **Such services are not required if, after an appropriate investigation, the person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached.**

Penalty

Pursuant to the enforcement duties and powers of the Director of Consumer Protection of the Department of Justice under Chapter 25 of Title 29, the Attorney General **may bring an action in law or equity** to address the violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both. The provisions of this chapter are not exclusive and do not relieve a person subject to this chapter from compliance with all other applicable provisions of law.

Nothing in this chapter may be construed to modify any right which a person may have at common law, by statute, or otherwise.

9. District of Columbia

D.C. Code §§ 28–3851 (2007)

What information is protected?

“Personal information” means either of the following:

- An individual’s first name or first initial and last name, or phone number, or address, and any one of the following data elements:
 - Social security number;
 - Driver’s license number or DC identification card; or
 - Credit card number or debit card number; or
- Any number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual’s financial or credit card account.

Notification of Breach

Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal

information, and who **discovers a breach of the security of the system**²³, shall promptly notify any District of Columbia resident whose personal information was included in the breach.

The notification shall be made **in the most expedient time possible and without unreasonable delay**, consistent with the legitimate needs of law enforcement, as provided in subsection (d) of this section, and with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

The notification required by this section **may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation** but shall be made as soon as possible after the law enforcement agency determines that the notification will not compromise the investigation.

Any person or entity who maintains, handles, or otherwise possesses computerized or other electronic data that includes personal information that the person or entity **does not own shall notify the owner** or licensee of the information of any breach of the security of the system in the most expedient time possible following discovery.

Requirements for Notification

“Notify” or “notification” means providing information through any of the following methods:

- Written notice;
- Electronic notice, if the customer has consented to receipt of electronic notice consistent with 15 U.S.C. 7001;
- Substitute notice, if the person or business demonstrates that the cost of providing notice to persons subject to this subchapter would exceed **\$50,000**, that the number of persons to receive notice under this subchapter exceeds **100,000**, or that the person or business does not have sufficient contact information. Substitute notice shall consist of the following:
 - Email notice when the person or business has an email address for the subject person;
 - Conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; and

²³ “Breach of the security of the system” means unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. The term “breach of the security system” shall not include a good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business if the personal information is not used improperly or subject to further unauthorized disclosure. **Acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party, shall not be deemed to be a breach of the security of the system.**

- Notice to major local and, if applicable, national media.

If any person or entity is required to notify **more than 1,000 persons** of a breach of security, the person shall also notify, without unreasonable delay, **all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis**, of the timing, distribution and content of the notices.

Penalty

Any District of Columbia resident injured by a violation of this subchapter may institute a civil action to recover **actual damages, the costs of the action, and reasonable attorney's fees**.

Actual damages **shall not** include dignitary damages, including pain and suffering.

The Attorney General may petition the Superior Court of the District of Columbia for temporary or permanent **injunctive relief** and for an award of **restitution for property lost or damages** suffered by District of Columbia residents as a consequence of the violation of this subchapter.

In an action under this subsection, the Attorney General may recover a civil penalty **not to exceed \$100 for each violation, the costs of the action, and reasonable attorney's fees**. Each failure to provide a District of Columbia resident with notification in accordance with this section shall constitute a separate violation.

The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

10. Florida

Fla. Stat. Ann. § 501.171 (2014)

Protection of Personal Information

Each covered entity,²⁴ governmental entity, or third-party agent shall take **reasonable measures to protect and secure data** in electronic form containing personal information.

Each covered entity or third-party agent shall take all reasonable measures to dispose, or arrange for the disposal, of customer records containing personal information within its custody or control when the records are no longer to be retained. Such disposal shall involve shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or

²⁴ "Covered entity" means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. For purposes of the notice requirements in subsections (3)-(6), the term includes a governmental entity.

undecipherable through any means.

What information is protected?

“Personal information” means either of the following:

- An individual’s first name or first initial and last name in combination with any one or more of the following data elements for that individual:
 - A social security number;
 - A driver’s license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identification;
 - A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual’s financial account;
 - Any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
 - An individual’s health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual;
- A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

Notification of Breach

A covered entity shall give notice to each individual in this state whose personal information was, or the covered **entity reasonably believes to have been, accessed as a result of the breach**²⁵.

Notice to individuals shall be made as **expeditiously as practicable and without unreasonable delay**, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, **but no later than 30 days after the determination of a breach or reason to believe a breach occurred** unless subject to a delay authorized by:

- If a federal, state, or local law enforcement agency determines that notice to individuals required under this subsection would interfere with a criminal investigation, the notice

²⁵ “Breach of security” or “breach” means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

shall be delayed upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably necessary;

Notice to the affected individuals **is not required if**, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that **the breach has not and will not likely result in identity theft or any other financial** harm to the individuals whose personal information has been accessed. Such a determination must be documented in writing and **maintained for at least 5 years**. The covered entity shall provide the **written determination** to the department **within 30 days after the determination**.

Third-parties: In the event of a breach of security of a system maintained by a third-party agent, such third-party agent shall notify the covered entity of the breach of security as **expeditiously as practicable**, but **no later than 10 days following the determination of the breach of security** or reason to believe the breach occurred. Upon receiving notice from a third-party agent, a covered entity shall provide notices required below. A third-party agent shall provide a covered entity with all information that the covered entity needs to comply with its notice requirements.

Requirements for Notification

In the case of a breach of personal information, notice is required to include to an **affected individual** by one of the following methods:

- Written notice sent to the mailing address of the individual in the records of the covered entity; or
- Email notice sent to the email address of the individual in the records of the covered entity.

The notice to an individual with respect to a breach of security shall include, at a minimum:

- The date, estimated date, or estimated date range of the breach of security.
- A description of the personal information that was accessed or reasonably believed to have been accessed as part of the breach of security.
- The information that the individual can use to contact the covered entity to inquire about the breach of security and the personal information that the covered entity maintained about the individual.
- Substitute notice, if
 - If such direct notice is not feasible because the cost of providing notice would exceed **\$250,000**, because the affected individuals exceed **500,000** persons, or

because the covered entity does not have an email address or mailing address for the affected individuals. Such substitute notice shall include the following:

- A conspicuous notice on the internet website of the covered entity if the covered entity maintains a website; and
- Notice in print and to broadcast media, including major media in urban and rural areas where the affected individuals reside.

Covered entities **must** provide **written** notice to the Florida Department of Legal Affairs of any breach of security affecting **500** or more individuals in the state. Such notice must be provided as **expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe a breach occurred.** A covered entity may receive 15 additional days for good cause. The written notice must include:

- A synopsis of the events surrounding the breach at the time notice is provided;
- The number of individuals in this state who were or potentially have been affected by the breach;
- Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions as to how to use such services;
- A copy of the notice sent to individuals or an explanation of the other actions taken pursuant to the statute;
- The name address, telephone number, and email address of the employee or agent of the covered entity from whom additional information may be obtained about the breach.

If a covered entity discovers circumstances requiring notice pursuant to this section of **more than 1,000 individuals** at a single time, the covered entity shall also notify, without unreasonable delay, **all consumer reporting agencies** that compile and maintain files on consumers on a nationwide basis

Penalty

A violation shall be treated as an unfair or deceptive trade practice in any action brought by the Florida Department of Legal Affairs against a covered entity or third-party agent.

In addition to the remedies available above, a covered entity shall be liable for a civil penalty not to exceed \$500,000, as follows:

- In the amount of \$1,000 for each day up to the first 30 days, and thereafter \$50,000 for each subsequent 30-day period or portion thereof for up to 180 days.
- If the violation continues for more than 150 days, in an amount not to exceed \$500,000.

The civil penalties for failure to notify provided above **apply per breach** and not per individual affected by the breach.

This section does not establish a private cause of action.

11. Georgia

Ga. Code Ann. §§ 10-1-910 (2005), as amended (2007)

What information is protected?

“Personal information” means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements **are not encrypted or redacted**:

- Social security number;
- Driver’s license number or state identification card number;
- Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords;
- Account passwords or personal identification numbers or other access codes; or
- Any of the items above when not in connection with the individual’s first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

Notification of Breach

Any information broker²⁶ or data collector²⁷ that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system **following discovery or notification** of the breach in the security of the data to any resident of this state whose **unencrypted personal information** was, or is reasonably believed to have been, acquired by an unauthorized person.

The notice shall be made in the most **expedient time possible and without unreasonable delay**, consistent with the legitimate needs of law enforcement, or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality

²⁶ “Information broker” means any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes.

²⁷ “Data collector” means any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity; provided, however, that the term “data collector” shall not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information.

of the data system.

Third-Party: Any person or business that maintains computerized data on behalf of an information broker or data collector that includes personal information of individuals that the person or business **does not own** shall notify the information broker or data collector of any breach of the security of the system **within 24 hours following discovery**, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Requirements for Notification

Notice means any of the following:

- Written notice;
- Telephone notice;
- Electronic notice, if the notice is consistent with 15 U.S.C. 7001; or
- Substitute notice, if the information broker or data collector demonstrates that the cost of providing notice would exceed **\$50,000.00**, that the affected class of individuals to be notified exceeds **100,000**, or that the information broker or data collector does not have sufficient contact information to provide written or electronic notice to such individuals. Substitute notice shall consist of the following:
 - Email notice, if the information broker or data collector has an email address for the individuals to be notified;
 - Conspicuous posting of the notice on the information broker's or data collector's website page, if the information broker or data collector maintains one; and
 - Notification to major state-wide media.

In the event that an information broker or data collector discovers circumstances requiring notification pursuant to this Code section of **more than 10,000 residents** of this state at one time, the information broker or data collector shall also notify, without unreasonable delay, **all consumer reporting agencies that compile and maintain files on consumers on a nation-wide basis**.

Penalty

No penalties are in place at the moment.

12. Guam

Guam Code Ann. tit. IX, §§ 48-10 (2009)

Protection of Personal Information

Both public and private entities on Guam have a duty to safeguard personal information that, if stolen or publicized, may result in crimes such as fraud and identity theft. The anonymity of the global internet, that transcends the borders of sovereign nations, makes it possible for unscrupulous individuals to profit from the theft of personal information and never be brought to justice for their crimes or made to pay restitution. Therefore, **it is incumbent upon all entities that are entrusted with such data to maintain strong security systems to ensure that the personal information will always be protected.**

What information is protected?

“Personal information” means:

- The first name, or first initial, and last name in combination with and linked to any one or more of the following data elements that relate to a resident of Guam, when the data elements are **neither encrypted nor redacted**:
 - Social security number;
 - Driver’s license number or Guam identification card number issued in lieu of a driver’s license; or
 - Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident’s financial accounts.

Notification of Breach

An individual *or* entity that owns *or* licenses computerized data that includes personal information **shall disclose** any breach of the security of the system²⁸ **following discovery *or* notification** of the breach of the security of the system to any resident of Guam whose **unencrypted and unredacted personal information was *or* is reasonably believed to have been accessed and acquired** by an unauthorized person and that causes, ***or* the individual *or* entity reasonably believes has caused *or* will cause, identity theft *or* other fraud to any resident of Guam.**, unless delayed by law enforcement because notice will impede a criminal investigation, *or* in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the disclosure **shall be made without unreasonable delay.**

An individual *or* entity must disclose the breach of the security of the system *if* encrypted **information** is accessed and acquired in an unencrypted form, *or if* the security breach involves a person with access to the encryption key and the individual *or* entity reasonably believes that such

²⁸ “Breach of the security of a system” means the unauthorized access and acquisition of **unencrypted and unredacted** computerized data that compromises the security *or* confidentiality of personal information maintained by an individual *or* entity as part of a database of personal information regarding multiple individuals and that **causes, *or* the individual *or* entity reasonably believes has caused *or* will cause, identity theft *or* other fraud to any resident of Guam.**

breach has caused *or* will cause identity theft *or* other fraud to any resident of Guam.

Third Party: An individual *or* entity that maintains computerized data that includes personal information that the individual *or* entity **does not own** or license **shall notify** the owner *or* licensee of the information of any breach of the security of the system **as soon as practicable following discovery**, *if* the personal information **was, or if the entity reasonably believes was, accessed and acquired by an unauthorized person**.

Requirements for Notification

Notice required by this section may be provided by:

- Written notice to the postal address in the records of the individual or entity;
- Telephone notice;
- Electronic notice; or
- Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed **ten thousand dollars**, or that the affected class of residents to be notified exceeds **five thousand** persons, or that the individual or the entity does not have sufficient contact information or consent to provide notice as described above. Substitute notice consists of any two of the following:
 - Email notice if the individual or the entity has email addresses for the members of the affected class of residents;
 - Conspicuous posting of the notice on the website of the individual or the entity, if the individual or the commercial entity maintains a website; and
 - Notice to major Guam media.

Penalty

The Office of the Attorney General *shall* have **exclusive authority** to bring action and may obtain either actual damages for a violation of this Chapter *or* a civil penalty *not to exceed* One Hundred Fifty Thousand Dollars (\$150,000) per breach of the security of the system *or* series of breaches of a similar nature that are discovered in a single investigation.

13. Hawaii

Haw. Rev. Stat. §§ 487N-1 (2006)

What information is protected?

“Personal information” means either of the following:

- An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are **not encrypted**:
 - Social security number;
 - Driver’s license number or Hawaii identification card number; or
 - Account number, credit or debit card number, access code, or password that would permit access to an individual’s financial account.

Notification of Breach

Any business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal information for specific government purposes **shall provide notice** to the affected person that there has been a security breach²⁹ **following discovery or notification of the breach**.

The disclosure notification shall be made **without unreasonable delay**, consistent with the legitimate needs of law enforcement, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data system.

Third-Party: Any business located in Hawaii or any business that conducts business in Hawaii that maintains or possesses records or data containing personal information of residents of Hawaii that the business does not own or license, or any government agency that maintains or possesses records or data containing personal information of residents of Hawaii shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subsection

Requirements for Notification

The notice provided to an individual shall be clear and conspicuous. The notice shall include a description of the following:

- The incident in general terms;

²⁹ “Security breach” means an incident of unauthorized access to and acquisition of **unencrypted or unredacted** records or data containing personal information **where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person**. Any incident of **unauthorized access** to and acquisition of **encrypted records** or data containing personal information **along with the confidential process or key constitutes a security breach**.

- The type of personal information that was subject to the unauthorized access and acquisition;
- The general acts of the business or government agency to protect the personal information from further unauthorized access;
- A telephone number that the person may call for further information and assistance, if one exists; and
- Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

Notice to affected persons may be provided by one of the following methods:

- Written notice to the last available address the business has on record;
- Electronic mail notice, if notice provided is consistent with 15 U.S.C. 7001;
- Telephone notice, provided that contact is made directly with the affected persons; and
- Substitute notice, if the business demonstrates that the cost of providing notice would exceed **\$100,000** or that the affected class of subject persons to be notified exceeds **two hundred thousand**, or if the business does not have sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of the following:
 - Electronic mail when the business or government agency has an email address for the subject person;
 - Conspicuous posting of the notice on the website page of the business or government agency, if one is maintained; and
 - Notification to major statewide media.

In the event a business provides notice to more than **one thousand persons** at one time pursuant to this section, the business **shall notify in writing, without unreasonable delay, the State of Hawaii's office of consumer protection and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.**

Penalty

Any business that violates any provision of this chapter shall be subject to penalties of not more than \$2,500 for each violation. The attorney general or the executive director of the office of consumer protection may bring an action pursuant to this section.

In addition, any business that violates any provision of this chapter shall be liable to the injured

party in an amount equal to the sum of any actual damages sustained by the injured party as a result of the violation. The court in any action brought under this section may award reasonable attorneys' fees to the prevailing party.

The penalties provided shall be cumulative to the remedies or penalties available under all other State laws.

14. Idaho

Idaho Code Ann. §§ 28-51-104 (2006)

What information is protected?

“Personal information” means the following:

- An Idaho resident’s first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when either the name or the data elements are **not encrypted**:
 - Social security number;
 - Driver’s license number or Idaho identification card number; or
 - Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident’s financial account.

Notification of Breach

A commercial entity³⁰ that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho shall, **when it becomes aware of a breach of the security of the system³¹, conduct in good faith a reasonable and prompt investigation** to determine the likelihood that personal information has been or will be misused.

If the investigation determines that the misuse of information about an Idaho resident has **occurred or is reasonably likely to occur**, the agency, individual or the commercial entity shall **give notice as soon as possible to the affected Idaho resident**.

Notice must be made in the most **expedient time possible and without unreasonable delay**.

³⁰ “Commercial entity” includes corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture and any other legal entity, whether for profit or not-for-profit.

³¹ “Breach of the security of the system” means the illegal acquisition of **unencrypted computerized data** that **materially compromises** the security, confidentiality, or integrity of personal information for one (1) or more persons maintained by a commercial entity.

consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system.

Third-Party: An agency, individual or a commercial entity that maintains computerized data that includes personal information that the agency, individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system **immediately following discovery of a breach** if misuse of personal information about an Idaho resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach.

Requirements for Notification

In the case of a breach of personal information, notice means:

- Written notice to the most recent address the agency, individual or commercial entity has in its records;
- Telephonic notice;
- Electronic notice, if the notice is consistent with 15 U.S.C. 7001;
- Substitute notice, if the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed **twenty-five thousand dollars**, or that the number of Idaho residents to be notified exceeds **fifty thousand**, or that the commercial entity does not have sufficient contact information to provide notice. Substitute notice consists of the following:
 - Email notice if the commercial entity has email addresses for the affected Idaho residents; and
 - Conspicuous posting of the notice on the website page of the agency, individual or the commercial entity if the agency, individual or the commercial entity maintains one; and
 - Notice to major statewide media.

Penalty

In any case in which a commercial entity's primary regulator has reason to believe that a commercial entity subject to that primary regulator's jurisdiction, has violated this section by failing to give notice in accordance with that section, the primary regulator may bring a **civil action** to enforce compliance with that section **and enjoin** that commercial entity from further violations.

Any commercial entity that intentionally fails to give shall be subject to a fine of not more than **twenty-five thousand dollars (\$25,000) per breach** of the security of the system.

15. Illinois

815 Ill. Comp Stat. Ann. 530/2 *et seq.*

What information is protected?

“Personal information” means either of the following:

- An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are **not encrypted or redacted or are encrypted or redacted but the keys to unencrypted or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security**:
 - Social security number;
 - Driver’s license number or State identification card number;
 - Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
 - Medical information;
 - Health insurance information;
 - Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;
- user name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer **are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security**.

Notification of Breach

Any data collector³² that owns or licenses personal information concerning an Illinois resident

³² “Data Collector” may include, but is not limited to, government agencies, public and private universities, **privately and publicly held corporations**, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

shall notify the resident at no charge that there has been a breach of the security of the system data³³ **following discovery or notification** of the breach.

The disclosure notification shall be made in **the most expedient time possible and without unreasonable delay**, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

Third Party: Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.

Requirements for Notification

In the case of a breach of **general** personal information, notice is required to include, but need not be limited to, information as follows:

- the toll-free numbers and addressed for consumer reporting agencies;
- the toll-free number, address, and website address for the Federal Trade Commission; and
- a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

For a breach of **username/email and password credentials**, notice may be provided in electronic or other form directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer.

Notice to consumers may be provided by one of the following methods:

- Written notice;

³³ “Breach of the security of the system data” or “breach” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector.

- Electronic notice, if the notice is consistent with 15 U.S.C. 7001; or
- Substitute notice, if the data collector demonstrates that the cost of providing notice would exceed \$250,000 or that the affected class of persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following:
 - Email notice if the data collector has an email address for the subject persons;
 - Conspicuous posting of the notice on the data collector's website page if the data collector maintains one; and
 - Notification to major statewide media or, if the breach impacts residents in one geographic area, to prominent local media in areas where affected individuals are likely to reside.

The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.

Penalty

A violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.

Violations are subject to a civil penalty of not more than \$100 for each individual with respect to whom personal information is disposed of in violation. A civil penalty may not exceed \$50,000 for each instance of improper disposal. The Attorney General may impose a civil penalty after notice to the person accused of violating this section. In addition, the Attorney General may bring an action in the circuit court to remedy a violation, seeking appropriate relief.

Note

IL S.B. 3007 was proposed on February 15, 2018, which would amend the Personal Information Protection Act and require a data collector required to issue to more than **100 Illinois residents** as a result of a single breach of security system shall provide notice to the Attorney General of the breach, including:

- A description of the nature of the breach of security or unauthorized acquisition or use;
- The number of Illinois residents affected by such incident at the time of notification;
- Any steps the data collector has taken or plans to take relating to the incident, including the steps the data collector has taken to inform the owner or licensee of the breach and what measures, if any, the data collector has taken to notify Illinois residents.

Such notice must be made within 14 business days of the data collector's discovery of the security breach.

16. Indiana

Ind. Code Ann. §§ 24–4.9, §§ 4–1–11 (2006), as amended (2009)

Protection of Personal Information

A data base owner³⁴ **shall implement and maintain reasonable procedures**, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner.

A data base owner shall not dispose of or abandon records or documents containing unencrypted and unredacted personal information of Indiana residents without shredding, incinerating, mutilating, erasing, or otherwise rendering the personal information illegible or unusable.

What information is protected?

“Personal information” means either of the following:

- A social security number that is **not encrypted or redacted**; or
- An individual’s first and last names, or first initial and last name, and one or more of the following data elements that are **not encrypted or redacted**:
 - A driver’s license number;
 - A state identification card number;
 - A credit card number;
 - A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person’s account.

Notification of Breach

After discovering or being notified of a breach of the security of data³⁵, the data base owner shall disclose the breach to an Indiana resident whose:

³⁴ “Data base owner” means a person that owns or licenses computerized data that includes personal information. “Person” means an individual, a corporation, a business trust, an estate, a trust, a partnership, an association, a nonprofit corporation or organization, a cooperative, or any other legal entity.

³⁵ “Breach of the security of data” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to **another medium, including paper, microfilm, or a similar medium**, even if the transferred data are no longer in a computerized format.

- **Unencrypted** personal information was or may have been acquired by an unauthorized person; or
- **Encrypted** personal information was or may have been acquired by an unauthorized person **with access to the encryption key**.

If the data base owner **knows, should know, or should have known** that the unauthorized acquisition constituting the breach has **resulted in or could result in identity deception, identity theft, or fraud** affecting the Indiana resident.

A person required to make a disclosure or notification under this chapter shall make the disclosure or notification **without unreasonable delay**. A delay is reasonable if the delay is:

- Necessary to restore the integrity of the computer system;
- Necessary to discover the scope of the breach; or
- In response to a request from the attorney general or a law enforcement agency to delay disclosure because disclosure will:
 - Impede a criminal or civil investigation; or
 - Jeopardize national security.

Third-Party: A person that maintains computerized data but that is not a data base owner shall notify the data base owner if the person discovers that personal information was or may have been acquired by an unauthorized person.

Requirements for Notification

In the case of a breach of personal information, a data base owner required to make a disclosure shall make the disclosure in one of the following methods:

- Mail;
- Telephone;
- Facsimile (fax);
- Electronic mail, if the data base owner has the electronic mail address of the affected Indiana resident;

- If a data base owner required to make disclosure to more than **five hundred thousand** Indiana residents, or if the data base owner required to make a disclosure determines that the cost of the disclosure will be more than **two hundred fifty thousand dollars**, the data base owner required to make a disclosure may elect to make the disclosure by using **both** of the following methods:
 - Conspicuous posting of the notice on the web site of the data base owner, if the data base owner maintains a website;
 - Notice to major news reporting media in the geographic area where Indiana residents affected by the breach of the security of a system reside.

A data base owner required to make a disclosure to more than **one thousand** (1,000) consumers **shall also disclose to each consumer reporting agency**, information necessary to assist the consumer reporting agency in preventing fraud, including personal information of an Indiana resident affected by the breach of the security of a system.

If a data base owner makes a disclosure to affected individuals, the data base owner **shall also disclose** the breach to the **attorney general**.

Penalty

A person that knowingly or intentionally fails to comply with any provision of this section commits a deceptive act that is **actionable only by the attorney general** under this section.

The attorney general may bring an action to obtain any or all of the following:

- An injunction to enjoin further violations;
- A civil penalty of not more than **five thousand dollars** per deceptive act;
- The attorney general's reasonable costs in:
 - The investigation of the deceptive act; and
 - Maintaining the action.

Failure to **implement and maintain** reasonable procedures or **disposing without shredding, incinerating, etc.** constitutes **one** deceptive act.

17. Iowa

Ia. Code Ann. §§ 715C.1 (2008), as amended (2014)

What information is protected?

“Personal information” means:

- An individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are **not encrypted, redacted, or otherwise altered** by any method or technology in such a manner that the name or data elements are unreadable **or** are **encrypted, redacted, or otherwise altered** by any method or technology **but the keys to unencrypt, unredact, or otherwise read the data elements have been obtained through the breach of security:**
 - Social security number;
 - Driver's license number or other unique identification number created or collected by a government body;
 - Financial account number, credit card number, or debit card number in combination with any required expiration date, security code, access code, or password that would permit access to an individual's financial account;
 - Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
 - Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

Notification of Breach

Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities and that was subject to a breach of security³⁶ **shall give notice** of the breach of security **following discovery of such breach of security** to any consumer whose personal information was included in the information that was breached.

The consumer notification shall be made in the **most expeditious manner possible and without unreasonable delay**, consistent with the legitimate needs of law enforcement, and consistent with any measures necessary to sufficiently determine contact information for the affected consumers, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data.

³⁶ “Breach of security” means unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. “Breach of security” also means unauthorized acquisition of personal information maintained by a person **in any medium, including on paper**, that was transferred by the person to that medium from computerized form and that compromises the security, confidentiality, or integrity of the personal information.

Notification is not required if, after an **appropriate investigation or after consultation** with the relevant federal, state, or local agencies responsible for law enforcement, the person determined that **no reasonable likelihood of financial harm** to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be **documented in writing** and the documentation must be **maintained for five years**.

Third-Party: Any person who maintains or otherwise possesses personal information on behalf of another person shall notify the owner or licensor of the information of any breach of security immediately following discovery of such breach of security if a consumer's personal information was included in the information that was breached.

Requirements for Notification

Notification shall include, at a minimum, all of the following:

- A description of the breach of security;
- The approximate date of the breach of security;
- The type of personal information obtained as a result of the breach of security;
- Contact information for consumer reporting agencies;
- Advise to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general.

Notification to the consumer may be provided by one of the following methods:

- Written notice to the last available address the person has in the person's records;
- Electronic notice if the person's customary method of communication with the consumer is by electronic means or is consistent with 15 U.S.C. § 7001; or
- Substitute notice, if the person demonstrates that the cost of providing notice would exceed **two hundred fifty thousand dollars**, that the affected class of consumers to be notified exceeds **three hundred fifty thousand** persons, or if the person does not have sufficient contact information to provide notice. Substitute notice shall consist of the following:
 - Electronic mail notice when the person has an electronic mail address for the affected customers;
 - Conspicuous posting of the notice or a link to the notice on the internet site of the person if the person maintains an internet site;

- Notification to major statewide media.

Any person that was subject to a breach of security requiring notification to **more than five hundred residents** of this state **shall give written notice** of the breach of security **to the director of the consumer protection division of the office of the attorney general within five business days after giving notice of the breach of security to any consumer.**

Penalty

A violation of this chapter is an unlawful practice under Iowa's Consumer Fraud Statute. Consequences include damages for injury and a fine of up to \$40,000 per violation.

18. Kansas

Kan. Stat. Ann. §§ 50-7a01 (2006)

What information is protected?

“Personal information” means the following:

- A consumer's first name or first initial and last name linked to any one or more of the following data elements that relate to the consumer, when the data elements are **neither encrypted nor redacted**:
 - Social security number;
 - Driver's license number or state identification card number; or
 - Financial account number, or credit or debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account.

Notification of Breach

A person³⁷ that conducts business in this state that owns or licenses computerized data that includes personal information shall, **when it becomes aware** of any breach of the security³⁸ of the system, conduct in good faith **a reasonable and prompt investigation** to determine the likelihood that personal information has been or will be misused.

If the investigation determines that **the misuse of information has occurred or is reasonably**

³⁷ “Person” means any individual, partnership, **corporation**, trust, estate, cooperative, association, government, or governmental subdivision or agency or other entity.

³⁸ “Security breach” means the unauthorized access and acquisition of **unencrypted or unredacted computerized data** that compromises the security, confidentiality or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity **reasonably believes has caused or will cause**, identity theft to any consumer.

likely to occur, the person shall give notice **as soon as possible** to the affected Kansas resident.

Notice must be made in the **most expedient time possible and without unreasonable delay**, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

Third Party: An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the data following discovery of a breach, if the personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.

Requirements for Notification

In the case of a breach of personal information, notice means:

- Written notice;
- Electronic notice, if the notice provided is consistent with 15 U.S.C. § 7001;
- Substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed **\$100,000**, or that the affected class of consumers to be notified exceeds 5,000, or that the individual or the commercial entity does not have sufficient contact information to provide notice. Substitute notice means:
 - Email notice if the individual or the commercial entity has email addresses for the affected class of consumers;
 - Conspicuous posting of the notice on the website page of the individual or the commercial entity if the individual or the commercial entity maintains a website; and
 - Notification to major statewide media.

In the event that a person discovers circumstances requiring of **more than 1,000** consumers at one time, the person **shall also notify, without unreasonable delay, all consumer reporting agencies** that compile and maintain files on consumers on a nationwide basis, of the timing, distribution and content of the notices.

Penalty

For violations of this section, the attorney general is empowered to bring an action in law or equity to address violations of this section and for other relief that may be appropriate.

The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law.

19. Kentucky

Ken. Rev. Stat. § 365.732 (2014)

What information is protected?

“Personal identifiable information” means the following:

- An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when the name or data element **not redacted**:
 - Social security number;
 - Driver’s license number; or
 - Account number or credit card number, in combination with any required security code, access code, or password to permit access to an individual’s financial account.

Notification of Breach

Any information holder³⁹ shall disclose any breach of the security of the system,⁴⁰ **following discovery or notification** of the breach in the security of the data, to any resident of Kentucky whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The disclosure shall be made in the **most expedient time possible and without unreasonable delay**, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Third-Party: Any information holder that maintains computerized data that includes personally identifiable information that the information holder does not own shall notify the owner or licensee of the information of any breach of the security of the data as soon as reasonably practicable following discovery, if the personally identifiable information was, or is reasonably believed to have been, acquired by an unauthorized person.

Requirements for Notification

³⁹ “Information holder” means any person or business entity that conducts business in this state.

⁴⁰ “Breach of the security of the system” means unauthorized acquisition of **unencrypted and unredacted computerized data** that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals **that actually causes, or leads the information holder to reasonably believe has caused or will cause**, identity theft or fraud against any resident of the Commonwealth of Kentucky.

In the case of a breach of personal information, notice may be provided by one of the following methods:

- Written notice;
- Electronic notice, if the notice provided is consistent with 15 U.S.C. 7001;
- Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed **two hundred fifty thousand dollars**, or that the affected class of subject persons to be notified exceeds **five hundred thousand**, or the information holder does not have sufficient contact information. Substitute notice shall consist of the following:
 - Email notice, when the information holder has an email address for the subject persons;
 - Conspicuous posting of the notice on the information holder's internet website page, if the information holder maintains a website page; and
 - Notification to major statewide media.

If a person discovers circumstances requiring notification of more than **one thousand (1,000)** persons at one time, the person shall also notify, without unreasonable delay, **all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis**, of the timing, distribution, and content of the notices.

Penalty

No listed penalties pursuant to the statute.

Note (Proposed Legislation)

KY S.B. 248 was proposed on March 1, 2018, which would fundamentally amend the security and personal information statute and require companies to change policies and procedures in Kentucky. "Personally identifiable information" will be amended to include: user name or email address with a security code, tax identification number, state identification number or other identification number issued by the state, and health information. Additionally, the statute will require notice no later than **thirty-five** days following discovery of the breach. Such notice will also require a company to provide a copy of his or her consumer report from each nationwide consumer reporting agency.

Additionally, an information holder who owns or licenses the personal identifiable information of more than **one thousand** residents of Kentucky **shall** encrypt all personally identifiable information electronically transmitted or stored by that information holder. If it is **not stored electronically**, the information holder **shall develop, implement, and maintain alternative compensating controls** consistent with industry standards and an assessment of risk, to protect

the security, confidentiality, and integrity of the personally identifiable information.

20. Louisiana

La. Rev. Stat. §§ 51:3071 (2005)

L.A.C. 16:III.701

Protection of Personal Information

Any person⁴¹ that conducts business in the state or that owns or licenses computerized data that includes personal information **shall implement and maintain reasonable security procedures and practices** appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

Any person that conducts business in the state or that owns or licenses computerized data that includes personal information **shall take all reasonable steps to destroy or arrange for the destruction of the records within its custody or control** containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

What information is protected?

“Personal information” means:

- The first name or first initial and last name of an individual resident of Louisiana in combination with any one or more of the following data elements, when the name or the data element is **not encrypted or not redacted**:
 - Social security number;
 - Driver’s license number or state identification card number;
 - Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
 - Passport number;
 - Biometric data, which means data generated by automatic measurements of an individual’s biological characteristics, such as fingerprints, voice print, eye retina or iris, or other unique biological characteristic that is used by the owner or

⁴¹ “Person” is not defined.

licensee to uniquely authenticate an individual's identity when the individual accesses a system or account.

Notification of Breach

Any person that owns or licenses computerized data that includes personal information shall, **following discovery of a breach in the security system⁴² containing such data**, notify any resident of the state whose personal information **was, or is reasonably believed to have been**, acquired by an authorized person.

Third-Party: Any agency or person that maintains computerized data that includes personal information that the agency or person **does not own** shall notify the owner or licensee of the information if the personal information **was, or is reasonably believed to have been**, acquired by an unauthorized person through a breach of security of the system containing such data, following discovery by the agency or person of a breach of security of the system.

In either case, notification shall be made **in the most expedient time possible without unreasonable delay but not later than sixty days from the discovery of the breach**, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system. If there is a delay because of the situations described above, the person or agency **shall provide the attorney general** the reasons for the delay **in writing** within the **sixty day** notification period.

Notification **shall not be required** if after a reasonable investigation, the person or business determines that there is **no reasonable likelihood of harm to the residents of Louisiana**. The person or business shall retain a copy of the written determination and supporting documentation for five years from the date of discovery of the breach of the security system.

Requirements for Notification

In the case of a breach of personal information, notice may be provided by one of the following methods:

- Written notification;
- Electronic notification, if consistent with 15 U.S.C. 7001;
- Substitute notification, if an agency or person demonstrates that the cost of providing notification would exceed **one hundred thousand dollars**, or that the affected class of persons to be notified exceeds **one hundred thousand**, or the agency or person does not have sufficient contact information. Substitute notification shall consist of all of the following:

⁴² "Breach of the security system" means the compromise of the security, confidentiality, or integrity of computerized data that **results in, or there is a reasonable likelihood to result in**, the unauthorized acquisition of and access to personal information maintained by an agency or person.

- Email notification when the agency or person has an email address for the subject persons;
- Conspicuous posting of the notification on the internet site of the agency or person, if an internet site is maintained; and
- Notification to major statewide media.

When notice to Louisiana citizens is required, the person or agency shall provide **written notice** detailing the breach of security of the system **to the Consumer Protection Section of the Attorney General's Office**. Notice shall include the names of **all** Louisiana citizens affected by the breach. Notice to the attorney general shall be timely **if received within 10 days** of notice to Louisiana citizens.

Penalty

Failure to provide timely notice may be punishable by a fine not to exceed \$5,000 per violation. Each day notice is not received to the Consumer Protection Section of the Attorney General's Office shall be deemed a separate violation.

A civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's personal information.

A violation of this statute shall constitute an unfair act or practice. A violation allows the attorney general to bring an action for injunctive relief and request that the court impose a civil penalty against the person.

21. Maine

Me. Rev. Stat. Ann. tit. 10 §§ 1346 (2005); as amended (2006)

What information is protected?

“Personal information” means:

- An individual's first name, or first initial, and last name in combination with any one or more of the following data elements, when either the name or the data elements are **not encrypted or redacted**:
 - Social security number;
 - Driver's license number or state identification card number;
 - Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords;

- Account passwords or personal identification numbers or other access codes; or
- Any of the data elements above when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

Notification of Breach

If any person⁴³ who maintains computerized data that includes personal information **becomes aware** of a breach of the security of the system,⁴⁴ the person shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State **if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur.**

The notices required must be made as **expediently as possible and without unreasonable delay**, consistent with the legitimate needs of law enforcement (must notify within **seven** business days after law enforcement determines it will not compromise investigation) or with measures necessary to determine the scope of the security breach and restore the reasonable integrity, security and confidentiality of the data in the system.

Third Party: A 3rd-party entity that maintains, on behalf of a person, computerized data that includes personal information that the 3rd-party entity **does not own** shall notify the person maintaining personal information of a breach of the security of the system **immediately following discovery** if the personal information **was, or is reasonably believed to have been, acquired by an unauthorized person.**

Requirements for Notification

In the case of a breach of personal information, notice means:

- Written notice;
- Electronic notice, if consistent with 15 U.S.C. 7001; or
- Substitute notice, if the person maintaining personal information demonstrates that the cost of providing notice would exceed **5,000**, that the affected class of individuals to be notified exceeds **1,000** or that the person maintaining personal information does not have

⁴³ "Person" means an individual, partnership, **corporation**, limited liability company, trust, estate, cooperative, association or other entity, including agencies of State Government, the University of Maine System, the Maine Community College System, Maine Maritime Academy and private colleges and universities.

⁴⁴ "Breach of the security of the system" or "security breach" means unauthorized acquisition, release or use of an individual's computerized data that includes personal information that compromises the security, confidentiality or integrity of personal information of the individual maintained by a person.

sufficient contact information to provide written or electronic notices to the individuals. Substitute notice must consist of all of the following:

- Email notice, if the person has email addresses for the individuals to be notified;
- Conspicuous posting of the notice on the person's publicly accessible website, if the person maintains one; and
- Notification to major statewide media.

When notice of a breach of the security of the system is required, the **person shall notify** the appropriate state regulators within the Department of Professional and Financial Regulation, or if the person is not regulated by the department, the **Attorney General**.

If a person discovers a breach of the security of the system that requires notification to **more than 1,000** persons at a single time, the person shall also notify, **without unreasonable delay, consumer reporting agencies that compile and maintain files** on consumers on a nationwide basis. Notification must include the **date of the breach, an estimate of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be notified of the breach**.

Penalty

A person that violates this chapter commits a civil violation and is subject to one or more of the following:

- A fine of not more than \$500 per violation, up to a maximum of \$2,500 for each day the person is in violation of this chapter;
- Equitable relief; or
- Enjoinment from further violations of this chapter.

22. Maryland

Md. Code Ann., Com. Law §§ 14–3501 (2007); as amended (2017)

Protection of Personal Information

To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State **shall implement and maintain reasonable security procedures and practices** that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations.

A business that uses **a nonaffiliated third party as a service provider** to perform services for

the business and discloses personal information about an individual residing in the State under a written contract with the third party **shall require by contract that the third party implement and maintain reasonable security procedures and practices** that:

- Are appropriate to the nature of the personal information disclosed to the nonaffiliated third party; and
- Are reasonably designed to help protect the personal information from unauthorized access, use, modification, disclosure, or destruction.

When a business is destroying a customer's, an employee's, or a former employee's records that contain personal information of the customer, employee, or former employee, the business shall take reasonable steps to protect against unauthorized access to or use of the personal information, taking into account:

- The sensitivity of the records;
- The nature and size of the business and its operations;
- The costs and benefits of different destruction methods; and
- Available technology.

What information is protected?

“Personal information” means either of the following:

- An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are **not encrypted, redacted, or otherwise protected** by another method that renders the information **unreadable or unusable**:
 - A social security number, an individual taxpayer identification number, a passport number, or other identification number issued by the federal government;
 - A driver's license number or State Identification card number;
 - An account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account;
 - Health information, including information about an individual's mental health;
 - A health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer

or an employer that is self-insured, that permits access to an individual's health information; or

- Biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account; or
- A username or email address in combination with a password or security question and answer that permits access to an individual's email account.

Notification of Breach

A business that owns or licenses computerized data that includes personal information of an individual residing in the State, **when it discovers or is notified of a breach** of the security⁴⁵ of a system, shall conduct in good faith **a reasonable and prompt investigation** to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach.

- If, after the investigation is concluded, the business determines that the breach of the security of the system **creates a likelihood that personal information has been or will be misused**, the business **shall notify** the individual of the breach.
- The notification required **shall be given as soon as reasonably practicable**, but **not later than 45 days** after the business concludes the investigation.
- **If after the investigation** is concluded, **the business determines that notice is not required**, the business **shall maintain records** that reflect its determination **for 3 years** after the determination is made.

Third Party: A business that maintains computerized data that includes personal information of an individual residing in the State that the business does not own or license, **when it discovers or is notified of a breach** of the security of a system, **shall notify, as soon as practicable**, the owner or licensee of the personal information of the breach of the security of a system.

- The **notification** required shall be given as soon **as reasonably practicable, but not later than 45 days** after the business discovers or is notified of the breach of the security of a system.

⁴⁵ "Breach of the security of a system" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business.

- A business that is required to notify an owner or licensee of personal information of a breach of the security of a system **shall share with the owner or licensee information relative to the breach.**

The notification required above may be delayed:

- If a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security; or
- To determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system.

If notification is delayed, notification shall be given as soon as reasonably practicable, but not later than thirty days after law the enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security.

Requirements for Notification

Prior to giving notice to an affected individual, a business shall provide notice of a breach of security of a system to the **Office of the Attorney General**.

In the case of a breach of personal information, notice is required to include:

- To the extent possible, a description of the categories of information that were, or are reasonably believed to have been acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired;
- Contact information for the business making the notification, including the business' address, telephone number, and toll-free telephone number if one is maintained;
- The toll-free telephone numbers and addresses for the major consumer reporting agencies; and
- The toll-free telephone numbers, addresses, and website addresses for:
 - The Federal Trade Commission; and
 - The Office of the Attorney General; and
 - A statement that the individual can obtain information from these sources about steps the individual can take to avoid identify theft.

The notification required may be given:

- By written notice to the most recent address of the individual in the records of the business;
- By electronic mail to the most recent electronic mail address, if
 - The individual has expressly consented to receive electronic notice; or
 - The business conducts its business primarily through internet account transactions or the internet;
- By telephonic notice, to the most recent telephone number of the individual; or
- By substitute notice, if:
 - The business demonstrates that the cost of providing notice would exceed **\$100,000** or that the affected class of individuals to be notified exceeds 175,000; or
 - The business does not have sufficient contact information to give notice.
 - Substitute notice shall consist of
 - Electronically mailing the notice to an individual entitled to notification if the business has an electronic mail address to be notified;
 - Conspicuous posting of the notice on the website of the business; and
 - Notification to statewide media.

In the case of a breach of security of a system involving access to an individual's **email account** and no other information, the business may comply with the notification requirement by providing the notification in **electronic or other form** that directs the individual whose personal information has been breached promptly to:

- Change the individual's password and security question or answer, as applicable; or
- Take other steps appropriate to protect the email account with the business and all other online accounts for which the individual uses the same username or email and password or security question.

If a business is required to give notice of a breach to **1,000** or more individuals, the business shall notify, **without unreasonable delay**, each consumer reporting agency that compiles and maintains

files on consumers on a nationwide basis of the timing, distribution, and contents of the notices.

Penalty

A violation of this title is an unfair or deceptive trade practice, and is subject to the enforcement and penalty provision contained in the Annotated Code of Maryland, Commercial Law Title 13.

23. Massachusetts

Mass Gen. Laws Ann. Ch. 93H, §§ 1 (2007)

Protection of Personal Information

201 CMR 17.00:

Every person that owns or licenses personal information about a resident of the Commonwealth **shall develop, implement, and maintain a comprehensive information security program** that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:

- the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program;
- the amount of resources available to such person;
- the amount of stored data; and
- the need for security and confidentiality of both consumer and employee information.

The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

Obligations

Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

- **Security Officer:** Designating one or more employees to maintain the comprehensive information security program;
- **Identifying Risks:** Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where

necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:

- Ongoing employee training;
 - Employee compliance with policies and procedures; and
 - Means for detecting and preventing security system failures.
- **Security Policies:** Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.
- **Disciplinary Measures:** Imposing disciplinary measures for violations of the comprehensive security program rules.
- **Prevention:** Preventing terminated employees from accessing records containing personal information.
- **Third Party:** Oversee service providers by taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information and requiring third-party service providers **by contract** to implement and maintain such appropriate security measures for personal information.
- **Reasonable Restrictions:** Reasonable restrictions upon access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers.
- **Monitoring:** Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access and upgrading systems regularly.
- **Annual Review:** Reviewing the scope of the security measures at least annually.
- **Documentation:** Documenting responsive actions taken in connection with incidents, and mandatory post-incident review of events and actions taken to make changes in business practices.

Computer System Security Requirements

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically

feasible, shall have the following elements:

- Secure user authentication protocols including:
 - control of user IDs and other identifiers;
 - a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
 - control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
 - restricting access to active users and active user accounts only; and
 - blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
- Secure access control measures that:
 - restrict access to records and files containing personal information to those who need such information to perform their job duties; and
 - assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;
- Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.
- Reasonable monitoring of systems, for unauthorized use of or access to personal information;
- Encryption of all personal information stored on laptops or other portable devices;
- For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information;
- Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis;

- Education and training of employees on the proper use of the computer security system and the importance of personal information security.

What information is protected?

“Personal information” means the following:

- A resident’s first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident:
 - Social security number;
 - Driver’s license number or state-issued identification card number; or
 - Financial account number, or credit or debit card number, **with or without** any required security code, access code, personal identification number or password, that would permit access to a resident’s financial account.

Notification of Breach

A person or agency that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, **as soon as practicable and without unreasonable delay**, when such person or agency (1) **knows or has reason to know of a breach of security**⁴⁶ or (2) when the person or agency **knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose**.

Third Party: A person or agency that maintains or stores, **but does not own or license data** that includes personal information about a resident of the commonwealth, shall provide notice, **as soon as practicable and without unreasonable delay**, when such person or agency (1) **knows or has reason to know of a breach of security** or (2) when the person or **agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose**, to the owner or licensor in accordance with this chapter.

In addition to providing notice to the owner, such person or agency shall cooperate with the owner or licensor of such information. Such cooperation shall include, but not be limited to:

- Informing the owner or licensor of the breach of security or unauthorized acquisition or use,

⁴⁶ “Breach of security”, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth.

- The date or approximate date of such incident and the nature thereof, and
- Any steps the person or agency has taken or plans to take relating to the incident, except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets, or to provide notice to a resident that may have been affected by the breach of security or unauthorized acquisition or use.

Requirements for Notification

The notice provided to the resident shall include, but not be limited to:

- The consumer's right to obtain a police report;
- How a consumer requests a security freeze and how the necessary information to be provided when requesting the security freeze; and
- Any fees required to be paid to any of the consumer reporting agencies.

The notification **shall not** include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access of use.

Notice shall include:

- Written notice;
- Electronic notice, if notice provided is consistent with 15 U.S.C. 7001
- Substitute notice, if the person or agency required to provide notice demonstrates that the cost of providing written notice will exceed **\$250,000**, or that the affected class of Massachusetts residents to be notified exceeds **500,000** residents, or that the person or agency does not have sufficient contact information to provide notice. Substitute notice shall consist of the following:
 - Electronic mail notice, if the person or agency has electronic mail addresses for the members of the affected class;
 - Clear and conspicuous posting of the notice on the home page of the person or agency if the person or agency maintains a website; and
 - Publication in or broadcast through media or medium that provides notice throughout the commonwealth.

Notification must also be made to the attorney general and director of consumer affairs and business regulation. Upon receipt of notice, the director of consumer affairs and business regulation will identify any relevant consumer reporting agency or state agency that needs to be notified to the notifying party.

Notice provided to the attorney general, director of consumer affairs, and consumer reporting agencies or state agencies shall include, but not limited to:

- The nature of the breach of security or unauthorized acquisition or use;
- The number of residents of Massachusetts affected by such incident at the time of the notification; and
- Any steps the entity has taken or plans to take relating to the incident.

Penalty

The attorney general may bring an action against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate. The attorney general may seek injunctive relief, a \$5,000 penalty for each violation, and reasonable costs and attorney's fees. Mass. Gen. Laws Ann. Ch. 93A § 4.

24. Michigan

Mich. Comp. Laws Ann. §§ 445.63 (2006)

What information is protected?

“Personal information” means the following:

- The first name or first initial and last name linked to one or more of the following data elements of a resident of Michigan:
 - Social security number;
 - Driver's license number or state personal identification card number;
 - Demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts.

Notification of Breach

Unless the person or agency determines that the security breach ⁴⁷**has not or is not likely to cause substantial loss or injury to, or result in identity theft** with respect to, one or more

⁴⁷ “Breach of the security of a database” or “security breach” means the unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals.

residents of this state, a person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach, shall provide a notice of the security breach to each resident of this state who meets one or more of the following:

- That resident's **unencrypted and unredacted** personal information was accessed and acquired by an unauthorized person.
- That resident's personal information was accessed and acquired in **encrypted** form by a person with **unauthorized access to the encryption key**.

In **determining whether** a security breach is **not likely to cause substantial loss or injury to, or result in identity theft** with respect to, one or more residents of this state, a person or agency **shall act with the care an ordinarily prudent person** or agency in like position would exercise under similar circumstances.

Notice shall be provided **without unreasonable delay**, unless:

- A delay is necessary in order for the person or agency to take any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database. However, the agency or person shall provide the notice required under this subsection without unreasonable delay after the person or agency completes the measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database.
- A law enforcement agency determines and advises the agency or person that providing a notice will impede a criminal or civil investigation or jeopardize homeland or national security. However, the agency or person shall provide the notice required under this section without unreasonable delay after the law enforcement agency determines that providing the notice will no longer impede the investigation or jeopardize homeland or national security.

Third Party: Unless the person or agency determines that the security breach **has not or is not likely to cause substantial loss or injury to, or result in identity theft** with respect to, one or more residents of this state, a person or agency that maintains a database that includes data that the person or agency **does not own** or license that discovers a breach of the security of the database **shall provide a notice to the owner or licensor of the information** of the security breach.

Requirements for Notification

A notice provided shall be written or communicated in a clear and conspicuous manner and contain the following:

- Describe the security breach in general terms;
- Describe the type of personal information that is subject of the unauthorized access or use;
- Generally describe what the agency or person providing the notice has done to protect data from further security breaches;
- Include a telephone number where a notice recipient may obtain assistance or additional information;
- Remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft.

Notice may be provided by one or more of the following:

- Written notice sent to the recipient at the recipient's postal address;
- Written notice sent electronically to the recipient if any of the following are met:
 - The recipient has expressly consented to receive electronic notice;
 - The person or agency has an existing business relationship with the recipient that includes periodic electronic mail communications and based on those communications the person reasonably believes that it has the recipients current electronic mail address; or
 - The person or agency conducts its business primarily through internet account transactions or on the internet.
- If not otherwise prohibited by state or federal law, by telephone, if
 - The notice is not given in whole or in part by use of a recorded message;
 - The recipient has expressly consented to receive notice by telephone, or if the recipient has not expressly consented to receive notice by telephone, the person or agency also provides written or electronic notice if the notice by telephone does not result in a live conversation between the individual representing the person or

agency and the recipient within 3 business days after the initial attempt to provide telephonic notice.

- Substitute notice, if the person or agency demonstrates that the cost of providing notice will exceed **\$250,000** or that the person or agency has to provide notice to more than **500,000** residents of this state. A person provides substitute notice by doing all of the following:
 - Electronic mail for any of the residents in the state who are entitled to receive the notice;
 - Conspicuously posting the notice on their website; and
 - Notifying major statewide media. Shall include telephone number or a website address that a person may use to obtain additional assistance and information.

After a person or agency provides notice to affected individuals, the person or agency **shall notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis** of the security breach without **unnecessary delay**. A notification shall include the number of notices that the person or agency provided to the residents and the timing of those notices. This section does not apply if the person or agency is required to provide notice to **1,000 or fewer residents of the state**.

Penalty

A person that knowingly fails to provide any notice of a security breach required under this section may be ordered to pay a civil fine of not more than \$250.00 for each failure to provide notice. The attorney general or prosecuting attorney may bring an action to recover a civil find under this section.

The aggregate liability of a person for civil fines for multiple violations that arise from the same security breach shall not exceed \$750,000.

25. Minnesota

Minn. Stat. Ann. § 325E.61 (2005), as amended (2007)

What information is protected?

“Personal information” means the following:

- An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when the data element is **not secured by encryption or any other method of technology that makes electronic data unreadable or unusable, or was secured**

and the encryption key, password, or other means necessary for reading or using the data was also acquired:

- Social security number;
- Driver's license number of Minnesota identification card number; or
- Account number or credit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Notification of Breach

Any person or business that conducts business in this state, and that owns or licenses data that includes personal information, shall disclose any breach of the security of the system⁴⁸ **following discovery or notification of the breach in the security of the data** to any resident of this state **whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.**

The disclosure must be made in the **most expedient time possible and without unreasonable delay**, consistent with the legitimate needs of law enforcement, or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.

Third Parties: Any person or business that maintains data that includes personal information that the person or business **does not own shall notify** the owner or licensee of the information of any breach of the security of the data **immediately following discovery**, if the personal information **was, or is reasonably believed to have been, acquired by an unauthorized person.**

Requirements for Notification

Notice may be provided by one of the following methods:

- Written notice to the most recent available address the person or business has in its records;
- Electronic notice, if the person's primary method of communication with the individual is by electronic means, or if the notice provided is consistent with 15 U.S.C. 7001; or
- Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed **\$250,000**, or that the affected class of subject persons to be notified exceeds **500,000**, or the person or business does not have sufficient contact information. Substitute notice must consist of all of the following:

⁴⁸ "Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.

- Email notice when the person or business has an email address for the subject persons;
- Conspicuous posting of the notice on the website page of the person or business, if the person or business maintains one; and
- Notification to a major statewide media.

For breaches affecting over **500** people, consumer reporting agencies must be notified within **48 hours**. When notifying a consumer reporting agency, a person or business **must include** the **timing, distribution, and content of the notice** being sent to the Minnesota residents.

Penalty

The attorney general shall enforce this section by seeking injunctive relief and/or a civil penalty for the state not to exceed \$25,000.

26. Mississippi

Miss. Code Ann. § 75–24–29 (2011)

What information is protected?

“Personal information” means the following:

- An individual’s first name or first initial and last name in combination with any one or more of the following data elements:
 - Social security number;
 - Driver’s license number or state identification card number; or
 - An account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual’s financial account.

Notification of Breach

A person who conducts business in this state shall **disclose any breach of security⁴⁹ to all affected individuals**. The disclosure shall be made **without unreasonable delay**, subject to a law

⁴⁹ “Breach of security” means unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of this state when access to the personal information **has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable**.

enforcement investigation⁵⁰ and the completion of an investigation by the person to determine the nature and scope of the incident, to identify the affected individuals, or to restore the reasonable integrity of the data system.

Notification shall not be required if, after an appropriate investigation, the person **reasonably determines** that the breach **will not likely result in harm to the affected individuals**.

Third Party: Any person who conducts business in this state that maintains computerized data which includes personal information that the person **does not own** or license **shall notify the owner or licensee** of the information of any breach of the security of the data **as soon as practicable following its discovery, if the personal information was, or is reasonably believed to have been,** acquired by an unauthorized person for fraudulent purposes.

Requirements for Notification

Any notice required by this section may be provided by one of the following methods:

- Written notice;
- Telephone notice;
- Electronic notice, if the person's primary means of communication with the affected individuals is by electronic means or if the notice is consistent with 15 U.S.C. 7001; or
- Substitute notice, provided the person demonstrates that the cost of providing notice would exceed **five thousand dollars**, that the affected class of subject persons to be notified exceeds **five thousand individuals** or the person does not have sufficient contact information. Substitute notice shall consist of the following:
 - Electronic mail notice when the person has an electronic mail address for the affected individuals;
 - Conspicuous posting of the notice on the website of the person if the person maintains one; and
 - Notification to major statewide media, including newspapers, radio and television.

Penalty

Failure to comply with the requirements of this section shall constitute an unfair trade practice and shall be enforced by the Attorney General; however, nothing in this section may be construed to

⁵⁰ Any notification required by this section shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation or national security and the law enforcement agency has made a request that the notification be delayed. Any such delayed notification shall be made after the law enforcement agency determines that notification will not compromise the criminal investigation or national security and so notifies the person of that determination.

create **a private right of action.**

27. **Missouri**

Mo. Rev. Stat. § 407.1500 (2009)

What information is protected?

“Personal information” means the following:

- An individual’s first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are **not encrypted, redacted, or otherwise altered** by any method or technology in such a manner that the name or data elements are **unreadable or unusable**:
 - Social security number;
 - Driver’s license number or other unique identification number created or collected by a government body;
 - Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
 - Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
 - Medical information;⁵¹ or
 - Health insurance information.⁵²

Notification of Breach

Any person⁵³ that owns or licenses personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses personal information in any form of a

⁵¹ “**Medical information**”, any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

⁵² “**Health insurance information**”, an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual.

⁵³ “**Person**”, any individual, **corporation**, business trust, estate, trust, partnership, limited liability company, association, joint venture, **government**, governmental subdivision, governmental agency, governmental instrumentality, public corporation, or any other legal or commercial entity.

resident of Missouri shall provide notice to the affected consumer that there has been a breach of security⁵⁴ **following discovery or notification of the breach.** The disclosure notification shall be:

- Made **without unreasonable delay;**
- Consistent with the legitimate needs of law enforcement, as provided in this section; and
- Consistent with any measures necessary to determine sufficient contact information and to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

Third Party: Any person that maintains or possesses records or data containing personal information of residents of Missouri that the person **does not own or license,** or any person that conducts business in Missouri that maintains or possesses records or data containing personal information of a resident of Missouri that the person does not own or license, **shall notify the owner or licensee of the information of any breach of security immediately following discovery of the breach,** consistent with the legitimate needs of law enforcement as provided in this section.

Notification is not required if, after an appropriate investigation by the person or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determines that **a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach.** Such a determination **shall be documented in writing** and the documentation shall be maintained **for five years.**

Requirements for Notification

In the case of a breach of personal information, notice shall at a minimum include a description of the following:

- The incident in general terms;
- The type of personal information that was obtained as a result of the breach of security;
- A telephone number that the affected consumer may call for further information and assistance, if one exists;
- Contact information for consumer reporting agencies;
- Advice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports.

Notification to affected consumers shall be provided by one of the following methods:

⁵⁴ “**Breach of security**” or “**breach**”, unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information.

- Written notice;
- Electronic notice for those customers for whom the person has a valid email address and who have agreed to receive communications electronically, if the notice provided is consistent with 15 U.S.C. 7001;
- Telephonic notice, if such contact is made directly with the affected consumers; or
- Substitute notice, if
 - The person demonstrates that the cost of providing notice would exceed **one hundred thousand dollars**; or
 - The class of affected consumers to be notified exceeds **one hundred fifty thousand**; or
 - The person does not have sufficient contact information or consent to satisfy the above notification methods, for only those affected consumers without sufficient contact information or consent; or
 - The person is unable to identify particular affected consumers, for only those unidentifiable consumers.
- Substitute notice shall consist of all of the following:
 - Email notice when the person has an electronic mail address for the affected consumers;
 - Conspicuous posting of the notice of a link to the notice on the internet website of the person if the person maintains an internet website; and
 - Notification to major statewide media.

In the event a person provides notice to **more than one thousand consumers at one time** pursuant to this section, the person **shall notify, without unreasonable delay, the attorney general's office and all consumer reporting agencies** that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. Section 1681a(p), of the timing, distribution, and content of the notice.

Penalty

The **attorney general shall have exclusive authority** to bring an action to obtain actual damages for a **willful and knowing violation** of this section and may seek a **civil penalty not to exceed one hundred fifty thousand dollars per breach** of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

Note

On January 24, 2018, Missouri H.B 2264 was proposed. The Bill seeks to amend two key provisions of this statute. First, instead of reporting a breach “without unreasonable delay,” the amended statute will require notification **within forty-eight hours** of the discovery or notification of the breach. Additionally, the Bill will allow “**any other person**” to bring an action to obtain actual damages, not just the attorney general.

28. Montana

Mont. Code Ann. §§ 30–14–1701 (2005), as amended (2015)

Protection of Personal Information

A business shall take all **reasonable steps to destroy or arrange for the destruction of a customer's records** within its custody or control containing personal **information that is no longer necessary** to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable.

What information is protected?

“Personal information” means the following:

- An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are **not encrypted**:
 - Social security number;
 - Driver’s license number, state identification card number, or tribal identification card number;
 - Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
 - Medical record information;⁵⁵

⁵⁵ “Medical record information” means personal information that:

(a) relates to an individual's physical or mental condition, medical history, medical claims history, or medical treatment; and

(b) is obtained from a medical professional or medical care institution, from the individual, or from the individual's spouse, parent, or legal guardian.

- A taxpayer identification number; or
- An identity protection personal identification number issued by the U.S. IRS.

Notification of Breach

Any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information **shall disclose** any breach of the security⁵⁶ of the data system **following discovery or notification of the breach** to any resident of Montana **whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.**

The disclosure must be made **without unreasonable delay**, consistent with the legitimate needs of law enforcement, or consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Third Party: Any person or business that maintains computerized data that includes personal information that the person or business **does not own** **shall notify** the owner or licensee of the information of any breach of the security of the data system **immediately following discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person.**

Requirements for Notification

Notice may be provided by one of the following methods:

- Written notice;
- Electronic notice, if the notice provided is consistent with 15 U.S.C. 7001;
- Telephonic notice; or
- Substitute notice, if the person or business demonstrates that:
 - The cost of providing the notice would exceed **\$250,000**;
 - The affected class of subject persons to be notified exceeds **500,000**; or
 - The person or business does not have sufficient contact information.
- Substitute notice must consist of the following:

⁵⁶ “Breach of the security of the data system” means unauthorized acquisition of computerized data that **materially compromises** the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident.

- An electronic mail notice when the person or business has an electronic mail address for the subject persons; and
- Conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; or
- Notification to applicable local or statewide media.

Any person or business that is required to issue a notification pursuant to this section **shall simultaneously submit an electronic copy of the notification and a statement providing the date and method of distribution of the notification to the attorney general's consumer protection office**, excluding any information that personally identifies any individual who is entitled to receive notification. If a notification is made to more than one individual, a single copy of the notification must be submitted that indicates the number of individuals in the state who received notification.

Penalty

Whenever the department has reason to believe that a person has violated this part and that proceeding would be in the public interest, the department may bring an action in the name of the state against the person to restrain by temporary or permanent injunction or temporary restraining order the use of the unlawful method, act, or practice upon giving appropriate notice to that person. A violation of this part is a violation of Mont. Code Ann. § 30-14-103, and the penalties for a violation of this part are as provided in Mont. Code Ann. § 30-14-142, including a civil fine of not more than **\$10,000 for each violation**.

29. Nebraska

Neb. Rev. Stat. §§ 87-802 (2006), as amended (2016)

Protection of Personal Information

To protect personal information from unauthorized access, acquisition, destruction, use, modification, or disclosure, an individual or a commercial entity **that conducts business in Nebraska and owns, licenses, or maintains computerized data that includes personal information** about a resident of Nebraska **shall implement and maintain reasonable security procedures and practices** that are appropriate to the nature and sensitivity of the personal information owned, licensed, or maintained and the nature and size of, and the resources available to, the business and its operations, including safeguards that protect the personal information when the individual or commercial entity disposes of the personal information.

Third Party: An individual or commercial entity that discloses computerized data that includes personal information about a Nebraska resident **to a nonaffiliated, third-party service provider** shall **require by contract that the service provider implement and maintain reasonable security procedures and practices that:**

- Are appropriate to the nature of the personal information disclosed to the service provider; and
- Are reasonably designed to help protect the personal information from unauthorized access acquisition, destruction, use, modification, or disclosure.

What information is protected?

“Personal information” means either of the following:

- A Nebraska resident’s first name or first initial and last name in combination with one or more of the following data elements that relate to the resident if either the name or the data elements are **not encrypted, redacted, or otherwise altered** by any method or technology in such a manner that the name or data elements are **unreadable**:
 - Social security number;
 - Motor vehicle operator’s license number or state identification card number;
 - Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident’s financial account;
 - Unique electronic identification number or routing code, in combination with any required security code, access code, or password; or
 - Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation; or
- A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

Notification of Breach

An individual or a commercial entity that conducts business in Nebraska and that owns or licenses computerized data that includes personal information about a resident of Nebraska shall, **when it becomes aware of a breach of the security⁵⁷ of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be used for an unauthorized purpose.**

If the investigation determines that the use of information about a Nebraska resident for an

⁵⁷ Breach of the security of the system means the unauthorized acquisition of **unencrypted computerized data** that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity.

unauthorized purpose **has occurred or is reasonably likely to occur**, the individual or commercial entity shall give notice to the affected Nebraska resident. Notice shall be made **as soon as possible and without unreasonable delay**, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

Third Party: An individual or a commercial entity that maintains computerized data that includes personal information that the individual or commercial entity **does not own** or license **shall give notice to and cooperate with** the owner or licensee of the information of any breach of the security of the system **when it becomes aware of a breach if use** of personal information about a Nebraska resident **for an unauthorized purpose occurred or is reasonably likely to occur**.

Cooperation includes, but is not limited to, sharing with the owner or licensee information relevant to the breach, not including information proprietary to the individual or commercial entity.

Requirements for Notification

Notice to an affected individual means:

- Written notice;
- Telephonic notice;
- Electronic notice, if consistent with 15 U.S.C. 7001;
- Substitute notice, if the individual or commercial entity required to provide notice demonstrates that the cost of providing notice will exceed **seventy-five thousand dollars**, that the affected class of Nebraska residents to be notified exceeds **one hundred thousand residents**, or that the individual or commercial entity does not have sufficient contact information to provide notice. Substitute notice under this subdivision requires all of the following:
 - Electronic mail notice if the individual or commercial entity has electronic mail addresses for the members of the affected class of Nebraska residents;
 - Conspicuous posting of the notice on the website of the individual or commercial entity if the individual or commercial entity maintains a website; and
 - Notice to major statewide media outlets.

If notice of a breach of security of the system is required, the individual or commercial entity **shall also, not later than the time when notice is provided to the Nebraska resident, provide notice of the breach of security of the system to the Attorney General.**

Penalty

The attorney general may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a breach of security.

A violation of the statute's **security procedures and practices** shall be considered a violation of the Consumer Protection Act and any other law which provides for the implementation and enforcement of thereof. A violation of the statute's security procedures and practices **does not** give rise to a private cause of action.

30. Nevada

Nev. Rev. Stat. §§ 603A.010 (2006), as amended (2017)

Protection of Personal Information

A business that maintains records which contain personal information concerning the customers of the business **shall take reasonable measures to ensure the destruction of those records** when the business decides that it will **no longer maintain the records**.

A data collector⁵⁸ that maintains records which contain personal information of a resident of this State **shall implement and maintain reasonable security measures** to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.

Third Party: A contract for the disclosure of the personal information of a resident of this State which is maintained by a data collector **must include a provision** requiring the person to whom the information is disclosed **to implement and maintain reasonable security measures** to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.

What information is protected?

“Personal information” means the following:

- A natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are **not encrypted**:
 - Social security number;

⁵⁸ “Data collector” means any governmental agency, institution of higher education, **corporation**, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information.

- Driver's license number, driver authorization card number or identification card number;
 - Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account;
 - A medical identification number or a health insurance identification number;
 - A username, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account.
- The term does not include the last four digits of a social security number, the last four digits of a driver's license number, the last four digits of a driver authorization card number or the last four digits of an identification card number or publicly available information that is lawfully made available to the general public from federal, state or local governmental records.

Notification of Breach

Any data collector that owns or licenses computerized data which includes personal information **shall disclose** any breach of the security of the system⁵⁹ data **following discovery or notification** of the breach to any resident of this State **whose unencrypted personal information was, or is reasonably believed to have been,** acquired by an unauthorized person.

The disclosure must be made in the **most expedient time possible and without unreasonable delay,** consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data.

Third Party: Any data collector that maintains computerized data which includes personal information that the data collector **does not own** shall notify the owner or licensee of the information of any breach of the security of the system data **immediately following discovery if the personal information was, or is reasonably believed to have been,** acquired by an unauthorized person.

Requirements for Notification

The notification required by this section may be provided by one of the following methods:

- Written notification;

⁵⁹ "Breach of the security of the system data" means unauthorized acquisition of computerized data that **materially compromises** the security, confidentiality or integrity of personal information maintained by the data collector.

- Electronic notification, if consistent with 15 U.S.C. 7001;
- Substitute notice, if the data collector demonstrates that the cost of providing notification would exceed **\$250,000**, the affected class of subject persons to be notified exceeds **500,000** or the data collector does not have sufficient contact information. Substitute notification must consist of all of the following:
 - Notification by electronic mail when the data collector has electronic mail addresses for the subject persons;
 - Conspicuous posting of the notification on the internet website of the data collector, if the data collector maintains an internet website;
 - Notification to major statewide media.

If the data collector determines that notification is required to be given to more than **1,000** persons at any one time, the data collector **shall also notify, without unreasonable delay, any consumer reporting agency that compiles and maintains files on consumers on a nationwide basis,** of the time the notification is distributed and the content of the notification.

Penalty

A data collector that provides the notification required may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector. A data collector that prevails in such an action may be awarded damages which may include, without limitation, the reasonable costs of notification, reasonable attorney's fees and costs and punitive damages when appropriate. The costs of notification include, without limitation, labor, materials, postage and any other costs reasonably related to providing the notification.

If the attorney general or district attorney of any county has reason to believe that any person is violating, proposes to violate or has violated these provisions, the attorney general or district attorney may bring an action against that person to obtain a temporary or permanent injunction against the violation.

31. New Hampshire

N.H. Rev. Stat. Ann. §§ 359-C:19 (2007)

What information is protected?

“Personal information” means the following:

- An individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are **not encrypted**:
 - Social security number;
 - Driver's license number or other government identification number;
 - Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Notification of Breach

Any person doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach⁶⁰, **promptly determine the likelihood that the information has been or will be misused**.

If the determination is that **misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made**, the person **shall notify** the affected individuals **as soon as possible**.

Notification **may be delayed** if a law enforcement agency, or national or homeland security agency determines that the notification will impede a criminal investigation or jeopardize national or homeland security.

Third Parties: Any person or business that maintains computerized data that includes personal information that the person or business **does not own** shall notify and cooperate with the owner or licensee of the information of any breach of the security of the data **immediately following discovery, if the personal information was acquired by an unauthorized person**.

Cooperation includes sharing with the owner or licensee information relevant to the breach; except that such cooperation shall not be deemed to require the disclosure of confidential or business information or trade secrets.

Requirements for Notification

In the case of a breach of personal information, notice is required to include:

- A description of the incident in general terms;
- The approximate date of breach;

⁶⁰ "Security breach" means unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state.

- The type of personal information obtained as a result of the security breach;
- The telephonic contact information of the person subject to this section.

The notice required under this section shall be provided by one of the following methods:

- Written notice;
- Electronic notice, if the business' primary means of communication with affected individuals is by electronic means;
- Telephonic notice, provided that a log of each such notification is kept by the person or business who notifies affected persons;
- Substitute notice, if the person demonstrates that the cost of providing notice would exceed **\$5,000**, that the affected class of subject individuals to be notified exceeds **1,000**, or the person does not have sufficient contact information or consent to provide the notice above. Substitute notice shall consist of the following:
 - Email notice when the person has an email address for the affected individuals;
 - Conspicuous posting of the notice on the person's business website, if the person maintains one;
 - Notification to major statewide media.

Any person engaged in trade or commerce shall also notify the regulator which has primary regulatory authority over such trade or commerce.

All other persons shall notify the New Hampshire attorney general's office. The notice shall include the anticipated date of the notice to the individuals and the approximate number of individuals in this state who will be notified.

If a person is required to notify more than **1,000** consumers of a breach of security, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the anticipated date of the notification to the consumers, the approximate number of consumers who will be notified, and the content of the notice.

Penalty

Any person injured by any violation under this subdivision may bring an action for damages and for such equitable relief, including an injunction, as the court deems necessary and proper. If the court finds for the plaintiff, recovery shall be in the amount of actual damages. If the court finds that the act or practice was a willful or knowing violation of this chapter, it shall award as much as 3 times, but not less than 2 times, such amount. In addition, a prevailing plaintiff shall be

awarded the costs of the suit and reasonable attorney's fees, as determined by the court. Injunctive relief shall be available to private individuals under this chapter without bond, subject to the discretion of the court.

The attorney general's office shall enforce these provisions by bringing an action in the name of the state to restrain the violation by temporary or permanent injunction, and to obtain up to \$10,000 in civil penalties for each violation.

32. New Jersey

N.J. Stat. Ann. § 56:8-161 (2006)

Protection of Personal Information

A business or public entity shall **destroy, or arrange for the destruction of**, a customer's records within its custody or control containing personal information, **which is no longer to be retained** by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or nonreconstructable through generally available means

What information is protected?

“Personal information” means the following:

- An individual's first name or first initial and last name linked with any one or more of the following data elements:
 - Social security number;
 - Driver's license number or state identification card number;
 - Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
 - Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

Notification of Breach

Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, **shall disclose** any breach of security⁶¹ of

⁶¹ Breach of security” means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal

those computerized records **following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person.**

The disclosure to a customer shall be made in **the most expedient time possible and without unreasonable delay**, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Disclosure of a breach of security to a customer **shall not be required** if the business or public entity establishes **that misuse of the information is not reasonably possible**. Any determination shall be **documented in writing and retained for five years**.

Third Party: Any business or public entity that compiles or maintains computerized records that include personal information **on behalf of another business shall notify** that business or public entity, who shall notify its New Jersey customers a. of this section, of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.

Requirements for Notification

Prior to giving notice to an affected individual, any business or public entity required to disclose a breach of security of a customer's personal information **shall report** the breach of security and any information pertaining to **the breach to the Division of State Police in the Department of Law and Public Safety** for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities.

For purposes of this section, notice may be provided to an affected customer by one of the following methods:

- Written notice;
- Electronic notice, if consistent with 15 U.S.C. 7001;
- Substitute notice, if the business or public entity demonstrates that the cost of providing notice would exceed **\$250,000**, or that the affected class of subject persons to be notified exceeds **500,000**, or the business or public entity does not have sufficient contact information. Substitute notice shall consist of all of the following:
 - Email notice when the business or public entity has an email address;

information **has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.**

- Conspicuous posting of the notice on the internet website page of the business or public entity, if the business or public entity maintains one; and
- Notification to major statewide media.

In the event that a business discovers circumstances requiring notification pursuant to this section of **more than 1,000 persons at one time**, the business or public entity **shall also notify, without unreasonable delay, all consumer reporting agencies** that compile or maintain files on consumers on a nationwide basis distribution and content of the notices.

Penalty

It shall be an unlawful practice to willfully, knowingly, or reckless violate the act. Therefore, remedies under this chapter apply to violations of the data breach notification law.

Note

On May 10, 2018, New Jersey S.B. No. 52 was proposed. This Bill proposes amending the statute to include “username, email address, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account” to “personal information.” This would also include specific notification procedures for breaches pertaining to those specific types of personal information.

33. New Mexico

NM Stat § 57-12C-6 (2017)

Protection of Personal Information

A person that owns or licenses records containing personal identifying information of a New Mexico resident **shall arrange** for the **proper disposal**, *i.e.* shredding, erasing or otherwise modifying the personal identifying information contained in the records to make the personal identifying information unreadable or undecipherable, **when they are no longer reasonably needed for business purposes**.

A person that owns or licenses personal identifying information of a New Mexico resident **shall implement and maintain reasonable security procedures and practices** appropriate to the nature of the information to protect the personal identifying information from unauthorized access, destruction, use, modification or disclosure.

Third Party: A person that discloses personal identifying information of a New Mexico resident pursuant to **a contract with a service provider** shall **require by contract** that the service provider **implement and maintain reasonable security procedures and practices** appropriate to the nature of the personal identifying information and to protect it from unauthorized access, destruction, use, modification or disclosure.

What information is protected?

“Personal identifying information” means the following:

- An individual’s first name or first initial and last name in combination with one or more of the following data elements that relate to the individual, when the data elements are **not protected through encryption or redaction or otherwise rendered unreadable or unusable**:
 - Social security number;
 - Driver’s license number;
 - Government-issued identification number;
 - Account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to a person’s financial amount; or
 - Biometric data.

Notification of Breach

A person that owns or licenses elements that include personal identifying information of a New Mexico resident **shall provide notification** to each New Mexico resident whose personal identifying information is **reasonably believed to have been subject to a security breach**.⁶²

Notification shall be made **in the most expedient time possible, but not later than forty-five calendar days** following the **discovery** of the security breach.

Notification may be **delayed** for a law enforcement investigation or as necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system.

Notification is not required if, after an appropriate investigation, the person determines that the security breach **does not give rise to a significant risk of identity theft or fraud**.

Third Party: Any person that is licensed to maintain or possess computerized data containing personal identifying information of a New Mexico resident that the person **does not own or license** shall notify the owner or licensee of the information of **any security breach in the most expedient time possible, but not later than forty-five calendar days following the discovery of the breach**, subject to all of the limitations above.

⁶² “Security breach” means the unauthorized acquisition of **unencrypted computerized data, or of encrypted computerized data and the confidential process or key used to decrypt the encrypted computerized data**, that compromises the security, confidentiality or integrity of personal identifying information maintained by a person.

Requirements for Notification

In the case of a breach of personal information, notice is required to include:

- The name and contact information of the notifying person;
- A list of the types of personal identifying information that are **reasonably believed** to have been the subject of a security breach, if known;
- The date of the security breach, the estimated date of the breach or the range of dates within which the security breach occurred, if known;
- A general description of the security breach incident;
- The toll-free telephone numbers and addresses of the major consumer reporting agencies;
- Advice that directs the recipient to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach; and
- Advice that informs the recipient of the notification of the recipient's rights pursuant to the federal Fair Credit Reporting.

A person required to provide notification shall provide notice by:

- United States mail;
- Electronic notification, if the person required to make the notification primarily communicates with the New Mexico resident by electronic means or if consistent with 15 U.S.C. 7001;
- A substitute notification, if the person demonstrates that the cost of providing notification would exceed **one hundred thousand dollars**, the number of residents to be notified exceeds **fifty thousand**, or the person does not have on record a physical address or sufficient contact information for the residents that the person or business is required to notify. Substitute notification shall consist of:
 - Sending electronic notification to the email address of those residents for whom the person has a valid email address;
 - Posting notification of the security breach in a conspicuous location on the website of the person required to provide notification if the person maintains a website; and

- Sending written notification to the office of the attorney general and major media outlets in New Mexico.

A person required to issue notification of a security breach to more than **one thousand** New Mexico residents as a result of a **single breach** shall notify the office of the **attorney general and major consumer reporting agencies** that compile and maintain files on consumers on a nationwide basis, no later than **forty-five calendar days**, subject to the exceptions above.

A person required to notify **the attorney general shall notify the number of New Mexico residents** that received notification and shall provide a copy of the notification that was sent to affected residents within forty-five calendar days following discovery of the security breach, subject to the exceptions above.

Penalty

When the attorney general has reasonable belief that a violation has occurred, he/she may bring an action on the behalf of the individuals and in the name of the state alleging a violation of the act. A court may:

- Issue an injunction; and
- Award damages for actual costs or loss, including consequential financial loss.

If the court determines that a person knowingly or recklessly violated the statute, the court may impose a civil penalty of the greater of twenty five thousand dollars or, in the case of failed notification, ten dollars per instance of failed notification up to a maximum of one hundred fifty thousand dollars.

34. New York

N.Y. Gen. Bus. Law § 899-aa (2005)

What information is protected?

“Personal information” means any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person.

“Private information” shall mean:

- Personal information consisting of any information in combination with any one or more of the following data elements, which either the personal information or the data element is **not encrypted, or encrypted with an encryption key that has also been acquired:**
 - Social security number;
 - Driver’s license number or non-driver identification card number; or

- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Notification of Breach

Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information **shall disclose** any breach of the security⁶³ of the system **following discovery or notification** of the breach in the security of the system to any resident of New York state whose private information **was, or is reasonably believed to have been, acquired by a person without valid authorization.**

In determining whether information **has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization,** such business may consider the following factors, among others:

- Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
- Indications that the information has been downloaded or copied; or
- Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

The **disclosure shall be made in the most expedient time possible and without unreasonable delay,** consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

Third Party: Any person or business which maintains computerized data which includes private information which such person or business **does not own shall notify** the owner or licensee of the information of any breach of the security of the system **immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.**

Requirements for Notification

In the case of a breach of personal information, notice is required to include, regardless of method:

⁶³ "Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business.

- Contact information for the person or business making the notification;
- A description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

The notice required by this section shall be directly provided to the affected persons by one of the following methods:

- Written notice;
- Electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction;
- Telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or
- Substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed **two hundred fifty thousand dollars**, or that the affected class of subject persons to be notified exceeds **five hundred thousand**, or such business does not have sufficient contact information. Substitute notice shall consist of all of the following:
 - Email notice when such business has an email address for the subject persons;
 - Conspicuous posting of the notice on such business's website page, if such business maintains one; and
 - Notification to major statewide media.

In the event that any New York residents are to be notified, the person or business **shall notify the state attorney general, the department of state and the division of state police as to the timing, content and distribution of the notices and approximate number of affected persons**. Such notice shall be made without delaying notice to affected New York residents.

In the event that more than five **thousand New York residents are to be notified at one time**, the person or business **shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons**. Such notice shall be made without delaying notice to affected New York residents.

Penalty

The attorney general may bring an action in a court having jurisdiction to issue an injunction. The court may award damages for actual costs or losses incurred by a person entitled to notice. Whenever the court determines that a person or business violated this article **knowingly or recklessly**, the court may impose a civil penalty of the greater of \$5,000 or up to \$10 per instance of failed notification, provided that the latter amount shall not exceed \$150,000.

Any other lawful remedy available can be sought as long as such action is commenced within two years immediately after the date of the act complained of or the date of discovery of such act.

Note

On June 1, 2018, 2017 NY N.B. 6933 was proposed. This amendment will add many terms to the definition of “private information,” including account numbers that could be accessed without additional information, biometric information, username/email and password, and health information.

35. North Carolina

N.C. Gen. Stat. §§ 75–60 (2005), as amended (2009)

What information is protected?

“Personal information” means the following:

- A person’s first name or initial and last name, in combination with any one or more of the following:
 - Social security or employer taxpayer identification numbers;
 - Driver’s license, state identification card, or passport numbers;
 - Account number, credit or debit card number, in combination with security or access codes or passwords to an individual’s financial account;
 - Digital signature;
 - Biometric data;
 - Fingerprints;
 - Other information that would permit access to a person’s financial account or resources.

Personal information shall not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.

Notification of Breach

Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (**whether computerized, paper, or otherwise**) **shall provide** notice to the affected person that there has been a security breach⁶⁴ **following discovery or notification of the breach.**

The disclosure notification shall be made **without unreasonable delay**, consistent with the legitimate needs of law enforcement, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

Third Party: Any business that maintains or possesses records or data containing personal information of residents of North Carolina that the business **does not own** or license, or any business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business **does not own** or license **shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach**, consistent with the legitimate needs of law enforcement.

Requirements for Notification

In the case of a breach of personal information, notice is required to include:

- A description of the incident in general terms;
- A description of the type of personal information that was subject to the unauthorized access and acquisition;
- A description of the general acts of the business to protect the personal information from further unauthorized access;
- A telephone number for the business that the person may call for further information and assistance, if one exists;

⁶⁴ "Security breach". -- An incident of unauthorized access to and acquisition of **unencrypted and unredacted records or data** containing personal information where illegal use of the personal information **has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer**. Any incident of unauthorized access to and acquisition of **encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach**.

- Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports;
- The toll-free numbers and addresses for the major consumer reporting agencies; and
- The toll-free numbers, addresses, and website addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft.

Notice to affected persons may be provided by one of the following methods:

- Written notice;
- Electronic notice, for those persons for whom it has a valid email address and who have agreed to receive communications electronically if consistent with 15 U.S.C. 7001;
- Telephonic notice provided that contact is made directly with the affected persons;
- Substitute notice, if the business demonstrates that the cost of providing notice would exceed **two hundred fifty thousand dollars** or that the affected class of subject persons to be notified exceeds **500,000**, or if the business does not have sufficient contact information or consent to satisfy the aforementioned methods, for only those affected persons without sufficient contact information, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of the following:
 - Email notice when the business has an electronic mail address for the subject persons;
 - Conspicuous posting of the notice on the website page of the business, if one is maintained;
 - Notification to major statewide media.

The business **shall also notify without unreasonable delay the Consumer Protection Division of the Attorney General's Office** of:

- The nature of the breach, the number of consumers affected by the breach;
- Steps taken to investigate the breach, steps taken to prevent a similar breach in the future; and
- Information regarding the timing, distribution, and content of the notice.

In the event a business provides notice to **more than 1,000 persons at one time**, the business **shall notify, without unreasonable delay, the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies** that compile and maintain files on consumers on a nationwide basis and content of the notice.

Penalty

An individual **injured or the attorney general** as a result of a violation of this section may institute a civil action. Damages set at \$5,000 per incident, and provides for treble damages with this range and attorney's fees. Injunctive relief is also available.

36. North Dakota

N.D. Cent. Code §§ 51-30-01 (2005), as amended (2015)

What information is protected?

“Personal information” means the following:

- An individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are **not encrypted**:
 - The individual's social security number;
 - The operator's license number assigned to an individual by the Department of Transportation;
 - A non-driver color photo identification card number assigned to the individual by the Department of Transportation;
 - The individual's financial institution account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts;
 - The individual's date of birth;
 - The maiden name of the individual's mother;
 - Medical information;
 - Health insurance information;
 - An identification number assigned to the individual by the individual's employer in combination with any required security code, access code, or password; or

- The individual's digitized or other electronic signature.

Notification of Breach

Any person that owns or licenses computerized data that includes personal information, **shall disclose** any breach of the security system⁶⁵ **following discovery or notification** of the breach in the security of the data to any resident of the state **whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.**

The disclosure must be made in the **most expedient time possible and without unreasonable delay**, consistent with the legitimate needs of law enforcement, or measures necessary to determine the scope of the breach and to restore the integrity of the data system.

Third Party: Any person that maintains computerized data that includes personal information that the person **does not own** **shall notify the owner or licensee** of the information of the breach of the security of the data **immediately following the discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.**

Requirements for Notification

Notice may be provided by one of the following methods:

- Written notice;
- Electronic notice, if consistent with 15 U.S.C. 7001;
- Substitute notice, if the person demonstrates that the cost of providing notice would **exceed two hundred fifty thousand dollars**, or that the affected class of subject persons to be notified **exceeds five hundred thousand**, or the person does not have sufficient contact information. Substitute notice consists of the following:
 - Electronic mail notice when the person has an electronic mail address for the subject persons;
 - Conspicuous posting of the notice on the person's website page, if the person maintains one; and
 - Notification to major statewide media.

In addition, any person that experiences a breach of the security system as provided in this section **shall disclose to the attorney general by mail or electronic mail any breach** of the security

⁶⁵ "Breach of the security system" means unauthorized acquisition of computerized data when access to personal information **has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable.**

system **which exceeds two hundred fifty individuals.**

Penalty

The attorney general may impose a civil penalty of not more than \$5,000 for each violation including attorney's fees, investigation fees, costs, and expenses of investigation. The remedies, duties, prohibitions, and penalties under this particular law are not exclusive and are in addition to all other causes of action, remedies, and penalties.

37. Ohio

Ohio Rev. Code Ann. §§ 1349.19 (2006)

What information is protected?

"Personal information" means the following:

- An individual's name , consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are **not encrypted, redacted, or altered** by any method or technology in such a manner that the data elements are **unreadable**:
 - Social security number;
 - Driver's license number or state identification card number;
 - Account number or credit or debit card number, in combination with a linked to any required security code, access code, or password that would permit access to an individual's financial account.

Notification of Breach

Any person that owns or licenses computerized data that includes personal information **shall disclose** any breach of the security of the system, **following its discovery or notification of the breach of the security of the system,**⁶⁶ to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident.

The person shall make the disclosure **in the most expedient time possible but not later than**

⁶⁶ "Breach of the security of the system" means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, **reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state.**

forty-five days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities, and consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system.

Third Party: Any person that, on behalf of or at the direction of another person or on behalf of or at the direction of any governmental entity, **is the custodian of or stores computerized data** that includes personal information **shall notify** that other person or governmental entity **of any breach of the security of the system in an expeditious manner**, if the personal information **was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of this state.**

Requirements for Notification

A person may disclose or make a notification by any of the following methods:

- Written notice;
- Electronic notice, if the person's primary method of communication with the resident to whom the disclosure must be made is by electronic means;
- Telephone notice;
- Substitute notice, if the person required to disclose demonstrates that the person does not have sufficient contact information to provide notice in a manner described above, or that the cost of providing disclosure or notice to residents to whom disclosure or notification is required would exceed **two hundred fifty thousand dollars**, or that the affected class of subject residents to whom disclosure or notification is required exceeds **five hundred thousand persons**. Substitute notice under this division shall consist of the following:
 - Electronic mail notice if the person has an electronic mail address for the resident to whom the disclosure must be made;
 - Conspicuous posting of the disclosure or notice on the person's website, if the person maintains one;
 - Notification to major media outlets.

If a person discovers circumstances that require disclosure to **more than one thousand residents** of this state involved in **a single occurrence** of a breach of the security of the system, the person **shall notify, without unreasonable delay, all consumer reporting agencies** that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given by the person to the residents of this state.

Penalty

The attorney general may conduct an investigation and bring a civil action upon an alleged failure by a person to comply with the requirements of this section.

Upon a finding that a person or agency has failed to comply with the statute, the court shall impose a civil penalty as follows:

- \$1,000 for each day the agency or person has intentionally or recklessly failed to comply with the applicable section up to 60 days;
- \$5,000 for each day AFTER 60 days and up to 90 days that the agency or person has intentionally or recklessly failed to comply with the applicable section;
- \$10,000 for each day AFTER 90 days that the agency or person has intentionally or recklessly failed to comply with the applicable section.

The rights and remedies that are provided under this section are in addition to any other rights or remedies that are provided by law.

38. Oklahoma

Okla. Stat. tit. 24 § 161 (2008)

Protection of Personal Information

To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State **shall**

What information is protected?

“Personal information” means the following:

- The first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are **neither encrypted nor redacted**:
 - Social security number;
 - Driver’s license number or state identification card number issued in lieu of a driver’s license; or
 - Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to the financial accounts of a resident.

Notification of Breach

An individual or entity that owns or licenses computerized data that includes personal information **shall disclose** any breach of the security of the system⁶⁷ **following discovery or notification** of the breach of the security of the system to any resident of this state whose **unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause,** identity theft or other fraud to any resident of this state.

An individual or **entity must disclose** the breach of the security of the system if **encrypted information is accessed and acquired in an unencrypted form** or if the security breach involves a person with access to the encryption key and the individual or **entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of this state.**

The disclosure shall be made **without unreasonable delay.** Notice required by this section **may be delayed** if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation or homeland or national security. **Notice** required by this section **must be made without unreasonable delay** after the law enforcement agency determines that notification will **no longer impede the investigation or jeopardize national or homeland security.**

Third Party: An individual or entity that maintains computerized data that includes personal information that the individual or entity **does not own** or license **shall notify** the owner or licensee of the information of any breach of the security of the system **as soon as practicable following discovery, if the personal information was or if the entity reasonably believes was accessed and acquired by an unauthorized person.**

Requirements for Notification

Notice means any of the following:

- Written notice to the postal address on records of the individual or entity;
- Telephone notice;
- Electronic notice; or

⁶⁷ “Breach of the security of a system” means the unauthorized access and acquisition of **unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information** maintained by an individual or entity as part of a database of personal information regarding multiple individuals and **that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state.**

- Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed **fifty thousand dollars**, or that the affected class of residents to be notified exceeds **one hundred thousand** persons, or that the individual or the entity does not have sufficient contact information or consent to provide the notice above. Substitute notice consists of any two of the following:
 - Email notice if the individual or the entity has email addresses for the members of the affected class of residents;
 - Conspicuous posting of the notice on the internet website of the individual or the entity if the individual or the entity maintains a public internet website, or
 - Notice to major statewide media.

Penalty

A violation of this act that results in injury or loss to residents in this state may be enforced by the attorney general or district attorney in the same manner as an unlawful practice under the Oklahoma Consumer Protection Act.

The attorney general or district attorney shall have exclusive authority to bring action and may obtain either actual damages for a violation of this act or a civil penalty not to exceed **one hundred fifty thousand dollars** per breach of the security system or serious of breaches of a similar nature that are discovered in a single investigation.

Note

On February 6, 2017, OK S.B. 614 was proposed. This amendment seeks to include notification to financial institutions that issued a credit or debit card compromised by a breach. It also includes factors to be considered by the attorney general when calculating damages.

39. Oregon

Or. Rev. Stat. §§ 646A.602 (2007)

Protection of Personal Information

A person that owns, maintains or otherwise possesses, or has control over or access to, data that includes personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities **shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including safeguards that protect the personal information when the person disposes of the**

personal information.

What information is protected?

“Personal information” means the following:

- A consumer’s first name or first initial and last name in combination with any one or more of the following data elements, **if encryption, redaction or other methods** have not rendered the data elements **unusable** or if the data elements are **encrypted and the encryption key has been acquired**:
 - A consumer’s social security number;
 - A consumer’s driver’s license number or state identification card number issued by the Department of Transportation;
 - A consumer’s passport number or other identification number issued by the United States;
 - A consumer’s financial account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to a consumer’s financial account, or any other information or combination of information that a person reasonably knows or should know would permit access to the consumer’s financial account;
 - Data from automatic measurements of a consumer’s physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer’s identity in the course of a financial transaction or other transaction;
 - A consumer’s health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; and
 - Any information about a consumer’s medical history or mental or physical condition or about a health care professional’s medical diagnosis or treatment of the consumer.
- Any of the data elements or any combination of the data elements described above without the consumer’s first name or first initial and last name, if:
 - Encryption, redaction or other methods have not rendered the data element or combination of data elements unusable; and
 - The data element or combination of data elements would enable a person to commit identity theft against a consumer.

Notification of Breach

If a person owns, licenses or otherwise possesses personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities and that **was subject to a breach of security**⁶⁸ or if the person **received notice of a breach** of security from another person that maintains or otherwise possesses personal information on the person's behalf, the person shall give notice of the breach of security to the consumer to whom the personal information pertains.

A person that must give notice of a breach of security under this section shall give the notice in **the most expeditious manner possible, without unreasonable delay, but not later than 45 days after discovering** or receiving notification of the breach of security.

In providing the notice, the person shall undertake reasonable measures that are necessary to:

- Determine sufficient contact information for the intended recipient of the notice;
- Determine the scope of the breach of security; and
- Restore the reasonable integrity, security and confidentiality of the personal information.
- A person that must give notice of a breach of security under this section may delay giving the notice only if a law enforcement agency determines that a notification will impede a criminal investigation and if the law enforcement agency requests in writing that the person delay the notification.

A person does **not need to notify consumers of a breach of security if**, after an appropriate **investigation** or after consultation with relevant federal, state or local law enforcement agencies, **the person reasonably determines** that the consumers whose personal information was subject to the breach of security are **unlikely to suffer harm**. The **person must document** the determination in writing and maintain the documentation **for at least five years**.

Third Party: A person that maintains or otherwise possesses personal information **on behalf of another** person **shall notify the other person as soon as is practicable after discovering a breach of security**.

Requirements for Notification

In the case of a breach of personal information, notice is required to include:

⁶⁸ "Breach of security" means an unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that a person maintains.

- A description of the breach of security in general terms;
- The approximate date of the breach of security;
- The type of personal information that was subject to the breach of security;
- Contact information for the person that gave the notice;
- Contact information for national consumer reporting agencies; and
- Advice to the consumer to report suspected identity theft to law enforcement, including the Attorney General and the Federal Trade Commission.

A person that must give notice may notify the consumer of a breach of security by one of the following:

- In writing;
- Electronically, if the person customarily communicates with the consumer electronically or if the notice is consistent with 15 U.S.C. 7001;
- By telephone, if the person contacts the affected consumer directly; or
- With substitute notice, if the person demonstrates that the cost of notification otherwise would exceed **\$250,000** or that the affected class of consumers exceeds **350,000**, or if the person does not have sufficient contact information to notify affected consumers.

Substitute notice means:

- Posting the notice or a link to the notice conspicuously on the person's website if the person maintains a website; and
- Notifying major statewide television and newspaper media.

A person that owns or licenses personal information **shall provide to the Attorney General within a reasonable time at least one copy of any notice the person sends to consumers.**

The person **must also notify the Attorney General**, either in writing or electronically, if the number of consumers to whom the person must send the notice **exceeds 250**.

If a person discovers a breach of security that affects **more than 1,000 consumers**, the person **shall notify**, without unreasonable delay, **all consumer reporting agencies** that compile and maintain reports on consumers on a nationwide basis of the timing, distribution and content of the notice the person gave to affected consumers and shall include in the notice any police report number assigned to the breach of security.

Penalty

Compensation can be ordered by the state upon a finding that enforcement of the rights of consumers by private civil action would be so burdensome or expensive as to be impractical.

In addition to other penalties and enforcement provisions provided by law, any person who violates or who procures, aids, or abets in violation of the data breach notification law shall be subject to a penalty of not more than \$1,000 per violation, but no more than \$500,000 total, which shall be paid to the General Fund of the State Treasury.

40. Pennsylvania

73 Pa. Stat. Ann. §§ 2301 (2006)

What information is protected?

“Personal information” means the following:

- An individual’s first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are **not encrypted or redacted**:
 - Social security number;
 - Driver’s license number or a state identification card number issued in lieu of a driver’s license;
 - Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual’s financial account.

Notification of Breach

An entity that maintains, stores or manages computerized data that includes personal information **shall provide notice** of any breach of the security of the system **following discovery of the breach** of the security of the system⁶⁹ to any resident of this Commonwealth whose unencrypted and unredacted personal information **was or is reasonably believed to have been accessed and acquired by an unauthorized person**.

An entity **must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form**, if the security breach is linked to a breach of the security of the

⁶⁹ “Breach of the security of the system” means the unauthorized access and acquisition of computerized data that **materially compromises** the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity **reasonably believes has caused or will cause loss or injury** to any resident of this Commonwealth.

encryption or **if the security breach involves a person with access to the encryption key.**

The **notice shall be made without unreasonable delay** except when a law enforcement agency determines and advises the entity in writing that the notification will impede a criminal investigation or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay.

Third Party: A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.

Requirements for Notification

Notice may be provided by any of the following methods of notification:

- Written notice to the last known home address for the individual;
- Telephonic notice, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance;
- Email notice, if a prior business relationship exists and the person or entity has a valid email address for the individual;
- Substitute notice, if the entity demonstrates one of the following: the cost of providing notice would exceed **\$100,000**, the affected class of subject persons to be notified exceeds **175,000**, or the entity does not have sufficient contact information. Substitute notice shall consist of the following:
 - Email notice when the entity has an email address for the subject persons;
 - Conspicuous posting of the notice on the entity's internet website if the entity maintains one;
 - Notification to major statewide media.

When an entity provides notification under this act to **more than 1,000 persons at one time**, the entity **shall also notify, without unreasonable delay, all consumer reporting agencies** that compile and maintain files on consumers on a nationwide basis of the timing, distribution and number of notices.

Penalty

A violation of this act shall be deemed to be an unfair or deceptive act and the Office of the Attorney General shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this act.

Note

On March 12, 2018, 2017 PA H.B. was proposed. This Bill redefines “breach of security system” and incorporates a few more terms to the definition of “personal information.” The Bill would also require specific notification requirements to the consumers upon breach, as well as notification to the attorney general of same.

41. Puerto Rico

10 L.P.R.A. §§ 4051 (2005), as amended (2008)

What information is protected?

“Personal information” means:

- At least the name or first initial and the surname of a person, together with any of the following data so that an association may be established between certain information with another and in which the information is legible enough so that in order to access it there is no need to use a special cryptographic code:
 - Social security number;
 - Driver’s license number, voter’s identification or other official identification;
 - Bank or financial account numbers of any type with or without passwords or access code that may have been assigned;
 - Names of users and passwords or access codes to public or private information systems;
 - Medical information protected by the HIPAA;
 - Tax information;
 - Work related evaluations.

Notification of Breach

Any entity that is the owner or custodian of a database that includes personal information of citizens residents of Puerto Rico **must notify** said citizens of any breach of the security of the

system⁷⁰ when the database **whose security has been breached contains, in whole or in part, personal information files and the same are not protected by an encrypted code but only by a password.**

Clients must be **notified as expeditiously as possible**, taking into consideration the need of law enforcement agencies to secure possible crime scenes and evidence as well as the application of measures needed to restore the system's security. Within a non-extendable term of ten (10) days after the violation of the system's security has been detected, the parties responsible shall inform the Department of Consumer Affairs, which shall make a public announcement of the fact within twenty-four (24) hours after having received the information.

Third Party: Any entity that as part of their operations resells or provides access to digital data banks that at the same time contain personal information files of citizens must notify the proprietor, custodian or holder of said information of any violation of the system's security that has allowed access to those files to unauthorized persons.

Requirements for Notification

The notice of breach of the security of the system shall be submitted in a clear and conspicuous manner and should:

- Describe the breach of the security of the system in general terms and the type of sensitive information compromised;
- The toll-free number and an internet site for people to use in order to obtain information or assistance.

To notify the citizens the entity shall have the following options:

- Written direct notice to those affected by mail or by authenticated electronic means according to the 15 U.S.C. 7001;
- When the cost of notifying all those potentially affected or of identifying them is excessively onerous due to the number of persons affected, to the difficulty in locating all persons or to the economic situation of the enterprise or entity; or whenever the cost exceeds one hundred thousand dollars or the number of person's exceeds one hundred thousand, the entity shall issue the notice through the following two steps:
 - (a) Prominent display of an announcement to that respect at the entities premises, on the web page of the entity, if any, and in any informative flier published and sent through mailing lists both postal and electronic, and (b) a communication to

⁷⁰ "Violation of the security system" means **any situation in which it is detected that access has been permitted to unauthorized persons or entities** to the data files so that the security, confidentiality or integrity of the information in the data bank has been compromised; or when normally authorized persons or entities have had access and it is known or there is reasonable suspicion that they have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information.

that respect to the media informing of the situation and providing information as to how to contact the entity to allow for better follow-up. When the information is of relevance to a specific professional or commercial sector, the announcement may be made through publications or programming of greater circulation oriented towards that sector.

A breach **shall be notified** to the **Citizen's Advocate Office**, which shall assume jurisdiction.

Penalty

The Secretary may impose fines of five hundred dollars (\$500) up to a maximum of five thousand dollars (\$5,000) for each violation of the provisions of this chapter or its regulations. The fines provided in this section do not affect the rights of the consumers to initiate actions or claims for damages before a competent court.

42. Rhode Island

R.I. Gen. Laws §§ 11-49.3-2 (2015)

Protection of Personal Information

A person⁷¹ that stores, collects, processes, maintains, acquires, uses, owns or licenses personal information about a Rhode Island resident **shall implement and maintain a risk-based information security program** that contains **reasonable security procedures and practices** appropriate to the size and scope of the organization; the nature of the information; and the purpose for which the information was collected in order to protect the personal information from unauthorized access, use, modification, destruction, or disclosure and to preserve the confidentiality, integrity, and availability of such information.

A person **shall not retain personal information for a period longer than is reasonably** required to provide the services requested; to meet the purpose for which it was collected; or in accordance with a written retention policy or as may be required by law. A municipal agency, state agency, or person shall destroy all personal information, regardless of the medium that such information is in, in a secure manner, including, but not limited to, shredding, pulverization, incineration, or erasure.

Third Party: A person who or that discloses personal information about a Rhode Island resident to a nonaffiliated third party **shall require by written contract** that **the third party implement and maintain reasonable security procedures and practices appropriate to** the size and scope of the organization; the nature of the information; and the purpose for which the information was collected in order to protect the personal information from unauthorized access, use, modification, destruction, or disclosure.

⁷¹ "Person" shall include any individual, sole proprietorship, partnership, association, **corporation**, joint venture, business or legal entity, trust, estate, cooperative, or other commercial entity.

What information is protected?

“Personal information” means the following:

- An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when the name and the data elements are **not encrypted or are in hard copy, paper format**:
 - Social security number;
 - Driver’s license number, Rhode Island identification card number, or tribal identification number;
 - Account number, credit, or debit card number, in combination with any required security code, access code, password, or personal identification number, that would permit access to an individual’s financial account;
 - Medical or health insurance information; or
 - Email address with any required security code, access code, or password that would permit access to an individual’s personal, medical, insurance, or financial account.

Notification of Breach

Any municipal agency, state agency, or person that stores, owns, collects, processes, maintains, acquires, uses, or licenses data that includes personal information **shall provide notification** as of **any disclosure of personal information, or any breach of the security of the system**,⁷² that **poses a significant risk of identity theft** to any resident of Rhode Island whose personal information **was, or is reasonably believed to have been, acquired by an unauthorized person or entity**.

The notification shall be made **in the most expedient time possible, but no later than forty-five (45) calendar days** after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements, and shall be consistent with the legitimate needs of law enforcement (**notice as soon as practicable** if law enforcement delays notice).

Requirements for Notification

In the case of a breach of personal information, notice is required to include:

- A general and brief description of the incident, including how the security breach occurred and the number of affected individuals;

⁷² “Breach of the security of the system” means unauthorized access or acquisition of **unencrypted, computerized data information** that compromises the security, confidentiality, or integrity of personal information maintained by the municipal agency, state agency, or person.

- The type of information that was subject to the breach;
- Date of breach, estimated date of breach, or the date range within which the breach occurred;
- Date that the breach was discovered;
- A clear and concise description of any remediation services offered to affected individuals including toll free numbers and websites to contact: (i) the credit report agencies, (ii) remediation service providers, and (iii) the attorney general;
- A clear and concise description of the consumer's ability to file or obtain a police report; how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze;; and that fees may be required to be paid to the consumer reporting agencies.

For purposes of this section, notice may be provided by one of the following methods:

- Written notice;
- Electronic notice, if consistent with 15 U.S.C. 7001; or
- Substitute notice, if the person demonstrates that the cost of providing notice would exceed **twenty-five thousand dollars**, or that the affected class of subject person to be notified exceeds **fifty thousand**, or the person does not have sufficient contact information. Substitute notice shall consist of all of the following:
 - Email notice when the person has an email address for the subject persons;
 - Conspicuous posting of the notice on the person's website page, if the person maintains one; and
 - Notification to major statewide media.

In the event that **more than five hundred (500) Rhode Island residents are to be notified**, the municipal agency, state agency, or person **shall notify the attorney general and the major credit reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected individuals**. Notification to the attorney general and the major credit reporting agencies shall be made without delaying notice to affected Rhode Island residents.

Penalty

Each reckless violation is a civil violation for which a penalty of not more than one hundred dollars per record may be adjudged against a defendant.

Each knowing and willful violation is a civil violation for which a penalty of not more than two hundred per record may be adjudged against a defendant.

Whenever the attorney general has reason to believe that a violation has occurred and the proceedings would be in the public interest, the attorney general may bring an action in the name of the state against the business or person in violation.

43. South Carolina

S.C. CODE § 39–1–90 (2009)

What information is protected?

“Personal identifying information” means:

- The first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this State, when the data elements are **neither encrypted nor redacted**:
 - Social security number;
 - Driver’s license number or state identification card number issued instead of a driver’s license;
 - Financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident’s financial account; or
 - Other numbers or information which may be used to access a person’s financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual.

Notification of Breach

A person conducting business in this State, and owning or licensing computerized data or other data that includes personal identifying information, **shall disclose** a breach of the security of the system⁷³ **following discovery or notification** of the breach in the security of the data to a resident of this State **whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person** when the illegal use of the information **has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident**.

The disclosure must be made **in the most expedient time possible and without unreasonable**

⁷³ “Breach of the security of the system” means unauthorized access to and acquisition of **computerized data that was not rendered unusable through encryption, redaction, or other methods** that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a **material risk of harm to a resident**.

delay, consistent with the legitimate needs of law enforcement, or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Third Party: A person conducting business in this State and maintaining computerized data or other data that includes personal identifying information that the person **does not own shall notify the owner or licensee of the information of a breach of the security of the data immediately following discovery, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.**

Requirements for Notification

Notice required by this section may be provided by:

- Written notice;
- Electronic notice, if the person's primary method of communication with the individual is by electronic means or is consistent with 15 U.S.C. 7001;
- Telephonic notice; or
- Substitute notice, if the person demonstrates that the cost of providing notice exceeds **two hundred fifty thousand dollars** or that the affected class of subject persons to be notified exceeds **five hundred thousand** or the person has insufficient contact information. Substitute notice consists of:
 - Email notice when the person has an email address for the subject persons;
 - Conspicuous posting of the notice on the website page of the person, if the person maintains one; or
 - Notification to major statewide media.

If a business provides notice to **more than one thousand persons** at one time pursuant to this section, the business **shall notify, without unreasonable delay, the Consumer Protection Division of the Department of Consumer Affairs and all consumer reporting agencies** that compile and maintain files on a nationwide basis of the timing, distribution, and content of the notice.

Penalty

A resident of this State who is injured by a violation of this section, in addition to and cumulative of all other rights and remedies available at law, may:

- Institute a civil action to recover damages in case of a willful and knowing violation;
- Institute a civil action that must be limited to actual damages resulting from a violation in case of a negligent violation of this section;

- Seek an injunction to enforce compliance; and
- Recover attorney's fees and court costs, if successful.

A person who knowingly and willfully violates this section is subject to an administrative fine in the amount of one thousand dollars for each resident whose information was accessible by reason of the breach, the amount to be decided by the Department of Consumer Affairs.

44. South Dakota

SENATE BILL 62 (2018)

What information is protected?

“Personal information” means the following:

- A person’s first name or first initial and last name, in combination with any one or more of the following elements:
 - Social security number;
 - Driver’s license number or other unique identification number created or collected by a government body;
 - Account, credit card, or debit card number, in combination with any required security code, access code, password, routing number, PIN, or any additional information that would permit access to a person’s financial account;
 - Medical information;
 - Health insurance information; or
 - An identification number assigned to a person by the person’s employer in combination with any required security code, access code, password, or biometric data generated from measurement or analysis of human body characteristics for authentication purposes.

“Protected information” means the following:

- A user name or email address, in combination with a password, security question answer, or other information that permits access to an online account; and
- Account number or debit card information, in combination with any required security code, or password that permits access to a person’s financial account.

Notification of Breach

Following the discovery or notification of a breach of system security an information holder⁷⁴ shall disclose the breach of system security⁷⁵ to any resident of this state whose personal or protected information **was, or is reasonably believed to have been, acquired by an unauthorized person.**

A **disclosure** under this section **shall be made not later than sixty days from the discovery or notification** of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement, but not later than **thirty days** after the law enforcement agency determines that notification will not compromise the criminal investigation.

An information holder is **not required to make a disclosure** under this section **if, following an appropriate investigation and notice to the attorney general, the information holder reasonably determines that the breach will not likely result in harm to the affected person.** The information holder **shall document** the determination under this section in writing and maintain the documentation **for not less than three years.**

Requirements for Notification

A disclosure under this section may be provided by:

- Written notice;
- Electronic notice, if consistent with U.S.C. 70001 or if the information holder's primary method of communication with the resident of the state has been by electronic means; or
- Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed **two hundred fifty thousand dollars**, that the affected class of persons to be notified exceeds **five hundred thousand persons**, or that the information holder does not have sufficient contact information and the notice consists of each of the following:
 - Email notice, if the information holder has an email address for the subject persons;
 - Conspicuous posting of the notice on the information holder's website, if the information holder maintains a website page; and
 - Notification to statewide media.

If an information holder discovers circumstances that require notification pursuant to regarding

⁷⁴ "Information holder," any person or business that conducts business in this state, and that owns or retains computerized personal or protected information of residents of this state.

⁷⁵ "Breach of system security," the acquisition of **unencrypted computerized data or encrypted computerized data and the encryption key** by an unauthorized person that materially compromises the security, confidentiality, or integrity of personal or protected information maintained by the information holder.

more than two hundred fifty persons at one time, the information holder **shall also notify, without unreasonable delay, all consumer reporting agencies** and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notice.

Any information holder that experiences a breach of system security under this section shall **disclose to the attorney general by mail or electronic mail** any breach of system security that **exceeds two hundred fifty residents of this state**.

Penalty

The attorney general may prosecute each failure to make a required disclosure as a deceptive act or practice. In addition, the attorney general may bring action to recover on behalf of the state a civil penalty of **not more than \$10,000 per day per violation**, and may recover attorney's fees and any accosts associate with any action brought under this title.

45. Tennessee

Tenn. Code Ann. §§ 47-18-2101 (2005); as amended (2016, 2017)

What information is protected?

“Personal information” means the following:

- An individual's first name or first initial and last name, in combination with any one or more of the following data elements:
 - Social security number;
 - Driver's license number; or
 - Account, credit card, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Notification of Breach

Following discovery or notification of a breach of system security⁷⁶ by an information holder,⁷⁷ the information holder shall disclose the breach of system security to any resident of this state

⁷⁶ “Breach of system security” means an acquisition of **unencrypted computerized data or encrypted computerized data and the encryption key** by an unauthorized person that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder.

⁷⁷ “Information holder” means any person or **business that conducts business in this state**, or any agency of this state or any of its political subdivisions, that owns or licenses computerized personal information of residents of this state.

whose personal information **was, or is reasonably believed to have been, acquired by an unauthorized person.**

The **disclosure** must be made **no later than forty-five (45) days from the discovery or notification** of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement, **but no later than forty-five days** after law enforcement determines that notification will not compromise the investigation.

Third Party: Any information holder that maintains computerized data that includes personal information that the information holder **does not own** shall notify the owner or licensee of the information of any breach of system security if the personal information **was, or is reasonably believed to have been, acquired by an unauthorized person.**

The **disclosure** must be made **no later than forty-five (45) days from the discovery or notification** of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement, **but no later than forty-five days** after law enforcement determines that notification will not compromise the investigation.

Requirements for Notification

Notice may be provided by one of the following methods:

- Written notice;
- Electronic notice, if consistent with 15 U.S.C. 7001 or if the information holder's primary method of communication with the resident of the state has been by electronic means; or
- Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed **two hundred fifty thousand dollars**, that the affected class of subject persons to be notified exceeds **five hundred thousand persons**, or if the information holder does not have sufficient contact information and the notice consists of all of the following:
 - Email notice, when the information holder has an email address for the subject persons;
 - Conspicuous posting of the notice on the information holder's website, if the information holder maintains a website page; and
 - Notification to major statewide media.

If an information holder discovers circumstances requiring notification of **more than one thousand (1,000) persons at one** time, the information holder must also notify, without unreasonable delay, **all consumer reporting agencies** and credit bureaus that compile and maintain files on consumers on a nationwide basis, of the timing, distribution, and content of the notices.

Penalty

Any customer of the information holder who is a person or business entity may institute a civil action to recover damages and enjoin the person or business entity from further action in violation of this statute. However, a customer cannot be an agency of the state or any political subdivision of the state.

In addition, a violation can subject the violator to a civil penalty of \$10,000, \$5,000 per day that a person's identity has been assumed, or 10 times the amount obtained or attempted to be obtained through the identity theft, whichever is greater. The attorney general can also seek injunctions and get attorney's fees. A violation under this statute may also be a violation of the Tennessee Consumer Protection Act.

46. Texas

Tex. Bus. & Com. Code §§ 521.001 (2007), as amended (2012)

Protection of Personal Information

A business shall **implement and maintain reasonable procedures**, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.

A business **shall destroy or arrange for the destruction** of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by shredding, erasing, or otherwise modifying the sensitive personal information in the records to make the information unreadable or indecipherable through any means.

What information is protected?

"Sensitive personal information" means the following:

- An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are **not encrypted**:
 - Social security number;
 - Driver's license number or government-issued identification number; or
 - Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
- Information that identifies an individual and relates to:

- The physical or mental health or condition of the individual;
- The provision of health care to the individual; or
- Payment for the provision of health care to the individual.

Notification of Breach

A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information **shall disclose** any breach of system security,⁷⁸ **after discovering or receiving notification** of the breach, to any individual whose sensitive personal information **was, or is reasonably believed to have been,** acquired by an unauthorized person.

The disclosure shall be **made as quickly as possible,** except a delay at the request of law enforcement that determines that the notification will impede a criminal investigation or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Third Party: Any person who maintains computerized data that includes sensitive personal information **not owned** by the person **shall notify** the owner or license holder of the information of any breach of system security **immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.**

Requirements for Notification

A person may give notice by providing:

- Written notice at the last known address of the individual;
- Electronic notice, if provided in accordance with 15 U.S.C. 7001; or
- Substitute notice, if the person demonstrates that the cost of providing notice would exceed **\$250,000**, the number of affected persons exceeds **500,000**, or the person does not have sufficient contact information, the notice may be given by:
 - Electronic mail, if the person has electronic mail addresses for the affected persons;
 - Conspicuous posting of the notice on the person's website; or
 - Notice published in a broadcast on major statewide media.

⁷⁸ "Breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, **including data that is encrypted if the person accessing the data has the key required to decrypt the data.**

If a person is required by this section to notify **at one time more than 10,000 persons** of a breach of system security, the person shall also notify each consumer reporting agency that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices. The person shall provide the notice required by this subsection without **unreasonable delay**.

Penalty

The attorney general may bring a civil suit for damages or an injunction. A person who violates the statute is liable to the state for a civil penalty of at least \$2,000 but no more than \$50,000 for each violation.

A person who fails to take reasonable action to comply with notification requirements is liable to the state for a civil penalty of not more than \$100 for each individual to whom notification is due for each consecutive day the person fails to take reasonable action to notify with a maximum penalty of \$250,000 for a single breach.

If it appears to the attorney general that a person is engaging in, has engaged in, or is about to engage in conduct that violates this chapter, the attorney general may bring an action in the name of the state against the person to restrain the violation by a temporary restraining order or by a permanent or temporary injunction.

The attorney general is entitled to recover reasonable expenses, including reasonable attorney's fees, court costs, and investigatory costs, incurred in obtaining injunctive relief or civil penalties, or both, under this section.

A violation of this statute is also a deceptive trade practice under the Texas Deceptive Trade Practices Act.

47. Utah

Utah Code Ann. §§ 13-44-101 (2006), as amended (2009)

Protection of Personal Information

Any person who conducts business in the state and maintains personal information **shall implement and maintain reasonable procedures** to:

- Prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business; and
- Destroy or arrange for the destruction (shredding, erasing, or otherwise modifying the personal information to make the information indecipherable) of records containing personal information that are not to be retained by the person.

What information is protected?

“Personal information” means the following:

- A person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person when **either the name or data element is unencrypted or protected by another method that renders the data unreadable or unusable:**
 - Social security number
 - Financial account number or credit or debit card number **and** any required security code, access code, or password that would permit access to the person's account; or
 - Driver's license number or state identification number.

Notification of Breach

A person who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the person **becomes aware of a breach of system security,**⁷⁹ **conduct** in good faith **a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes.**

If an investigation reveals that the misuse of personal information for identity theft or fraud purposes **has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident.**

A person required to provide notification shall provide the notification in **the most expedient time possible without unreasonable delay:**

- Considering legitimate investigative needs of law enforcement;
- After determining the scope of the breach of system security; and
- After restoring the reasonable integrity of the system.

Third Party: A person who maintains computerized data that includes personal information that the person **does not own** or license shall notify and cooperate with the owner or licensee of the information of any breach of system security **immediately following the person's discovery of the breach if misuse of the personal information occurs or is reasonably likely to occur.**

Requirements for Notification

⁷⁹ Breach of system security" means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information.

A person may give notice by providing:

- In writing by first-class mail to the most recent address the person has for the resident;
- Electronically, if the person's primary method of communication with the resident is by electronic means, or if provided in accordance with the consumer disclosure provisions of 15 U.S.C. 7001;
- By telephone, including though he use of automatic dialing technology not prohibited by other law; or
- By publishing notice of the breach of security system:
 - In a newspaper of general circulation and as required by Utah Code Ann. § 14-1-101.

Penalty

The statute does not give a private right of action, but likewise does not affect any private right of action that may exist under other law, including contract or tort.

A person who violates this subchapter is subject to a civil fine of: (a) No greater than \$2,500 for a violation of series of violations concerning a specific consumer; and (b) no greater than \$100,000 in the aggregate for related violations concerning more than one consumer.

The attorney general may also seek injunctive relief, attorney's fees, and costs.

48. Vermont

Vt. State. Ann. tit. 9, §§ 2430 (2006); as amended (2008, 2012)

What information is protected?

"Personally identifiable information" means the following:

- A consumer's first name or first initial and last name in combination with any one or more of the following digital data elements, when either the name or data elements **are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons:**
 - Social security number;
 - Motor vehicle operator's license number or non-driver identification card number;

- Financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords;
- Account passwords or personal identification numbers or other access codes for a financial account.

Notification of Breach

Any data collector⁸⁰ that owns or licenses⁸¹ computerized personally identifiable information that includes personal information concerning a consumer **shall notify** the consumer that there has been a security breach⁸² **following discovery or notification to the data collector of the breach.**

Notice of the security breach shall be **made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification,** consistent with the legitimate needs of the law enforcement agency or with any measures necessary to

⁸⁰ “Data collector” includes, but is not limited to, the state, state agencies, political subdivisions of the state, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, retail operators, and any other entity that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

(Effective January 1, 2019) “Data collector” means a person who, for any purpose whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with personally identifiable information, and includes publicly held corporation, LLCs, financial institutions, and retail operators.

⁸¹ (Effective January 1, 2019) “License” means a grant of access to, or distribution of, data by one person to another in exchange for consideration. A use of data for the sole benefit of the data provider, where the data provider maintains control over the use of the data, is not a license.

⁸² “Security breach” means unauthorized acquisition of, electronic data or a reasonable belief of an unauthorized acquisition of, electronic data that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information maintained by a data collector.

(C) In determining whether personally identifiable information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data collector may consider the following factors, among others:

- (i) indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information;
- (ii) indications that the information has been downloaded or copied;
- (iii) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or
- (iv) that the information has been made public

determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system.

Notice of a security breach is **not required** if the data collector establishes that **misuse of personal information is not reasonably possible** and the data collector provides notice of the determination and a detailed explanation for said determination to the Vermont attorney general or to the department of banking, insurance, securities, and health care administration. If the data collector later gathers facts to indicate that the misuse of personal information is reasonably possible, then the notice is required.

Third Party: Any data collector that maintains or possesses computerized data containing personally identifiable information of a consumer that the data collector **does not own** or license or any data collector that acts or conducts business in Vermont that maintains or possesses records or data containing personally identifiable information that the data collector does not own or license **shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach**, consistent with the legitimate needs of law enforcement.

Requirements for Notification

Notice to a consumer shall be clear and conspicuous. The notice shall include a description of each of the following, if known to the data collector:

- The incident in general terms;
- The type of personally identifiable information that was subject to the security breach;
- The general acts of the data collector to protect the personally identifiable information from further security breach;
- A telephone number, toll-free if available, that the consumer may call for further information and assistance;
- Advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports; and
- The approximate date of the security breach.

A person may give notice by providing one of the following:

- A direct notice, which may be one of the following:

- Written notice mailed to the consumer's residence;
- Electronic notice, for those consumers for whom the data collector has a valid email address if,
 - The data collector's primary method of communication with the consumer is by electronic means, the electronic notice does not request or contain a hypertext link to a request that the consumer provide personal information, and the electronic notice conspicuously warns consumers not to provide personal information in response to electronic communications regarding security breaches; or
 - The notice is consistent with 15 U.S.C. 7001; or
- Telephonic notice, provided that telephonic contact is made directly with each affected consumer and not through a prerecorded message.
- Substitute notice, if the data collector demonstrates that the cost of providing written or telephonic notice to affected consumers would exceed **\$5,000**, the class of affected consumers to be provided written or telephonic notice exceeds **5,000**; or the data collector does not have sufficient contact information. A data collector shall provide substitute notice by:
 - Conspicuously posting the notice on the data collector's website if the data collector maintains one; and
 - Notifying major statewide and regional media.

Once notice is made to consumers, **the attorney general must be notified** of the number of Vermont consumers affected and provide a copy of the notice. A second copy of the consumer notification letter, with personally identifiable information that was subject to the breach redacted, can also be provided to the attorney general which will be used for any public disclosure of the breach.

In the event a data collector provides notice to **more than 1,000** consumers at **one time**, the data collector shall notify, without unreasonable delay, all consumer reporting agencies. In notice to a consumer reporting agency, the data collector must include the timing, distribution, and content of the notices being sent to the affected consumers.

Penalty

The attorney general and state's attorney shall have sole and full authority to investigate potential violations and to enforce, prosecute, obtain, and impose remedies for any violation.

49. Virgin Islands

14 V.I.C. §§ 2208 (2005)

What information is protected?

“Personal identifying information” means:

- An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are **not encrypted**:
 - Social security number;
 - Driver’s license number;
 - Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

Notification of Breach

Any agency that owns or licenses computerized data that includes personal information **shall disclose** any breach of the security of the system⁸³ **following discovery or notification** of the breach in the security of the data to any resident of the Virgin Islands whose **unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person**.

The disclosure must be made in **the most expedient time possible and without unreasonable delay**, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Third Party: Any agency that maintains computerized data that includes personal information that the agency **does not own** shall notify the owner or licensee of the information of any breach of the security of the data **immediately following discovery**, if the personal information **was, or is reasonably believed to have been, acquired by an unauthorized person**.

Requirements for Notification

Notice required by this section may be provided by one of the following methods:

- Written notice;
- Electronic notice, if consistent with 15 U.S.C. 7001;

⁸³ Breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency.

- Substitute notice, if the agency demonstrates the cost of providing notice would exceed **\$100,000**, or that the affected class of subject persons to be notified exceeds **50,000**, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:
 - Email notice when the agency has an email address for the subject persons;
 - Conspicuous posting of the notice on the agency’s website page, if the agency maintains one;
 - Notification to major territory-wide media.

Penalty

Any customer injured by a violation of this title may commence a civil action to recover damages.

Any business that violates, proposes to violate or has violated this title may be enjoined.

The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

50. Virginia

1. Va. Code Ann. § 18.2-186.6 (2008) – General Personal Information

What information is protected?

“Personal information” means the following:

- The first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of a commonwealth, when the data elements are **neither encrypted nor redacted**:
 - Social security number;
 - Driver’s license number or state identification card number issued in lieu of a driver’s license number; or
 - Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident’s financial accounts.

Notification of Breach

If **unencrypted or unredacted** personal information **was or is reasonably believed** to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes **has caused or will cause**, identity theft or another fraud to any resident of the Commonwealth, an individual or entity that owns or licenses computerized data that includes personal information **shall disclose** any breach of the security of the system⁸⁴ **following discovery or notification** of the breach of the security of the system **to the Office of the Attorney General and any affected resident** of the Commonwealth **without unreasonable delay**.

An individual or entity **shall disclose** the breach of the security of the system **if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key** and the individual or entity **reasonably believes** that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth.

Notice required by this section may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system.

Notice required by this section may be delayed if, after the individual or entity notifies a law-enforcement agency, the law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

Third Party: An individual or entity that maintains computerized data that includes personal information that the individual or entity **does not own** or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay **following discovery of the breach of the security of the system**, if the personal information **was accessed and acquired** by an unauthorized person or the individual **or** entity **reasonably believes the personal information was accessed and acquired** by an unauthorized person.

Requirements for Notification

Notice required by this section shall include a description of the following:

- The incident in general terms;
- The type of personal information that was subject to the unauthorized access and acquisition;

⁸⁴ “Breach of the security of the system” means the unauthorized access and acquisition of **unencrypted and unredacted** computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that **causes, or the individual or entity reasonably believes has caused, or will cause**, identity theft or other fraud to any resident of the Commonwealth.

- The general acts of the individual or entity to protect the personal information from further unauthorized access;
- A telephone number that the individual may call for further information and assistance, if one exists; and
- Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

Notice means any of the following:

- Written notice to the last known postal address in the records of the individual or entity;
- Telephone notice;
- Electronic notice; or
- Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed **\$50,000**, the affected class of Virginia residents to be notified exceeds **100,000** residents, or the individual or the entity does not have sufficient contact information or consent to provide notice as described above.

Substitute notice consists of all of the following:

- Email notice if the individual or the entity has email addresses for the members of the affected class of residents;
- Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and
- Notice to major statewide media.

In the event an individual or entity provides notice to **more than 1,000 persons** at one time pursuant to this section, the individual or entity shall notify, without unreasonable delay, **the Office of the Attorney General and all consumer reporting agencies** that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notice.

Penalty

The Attorney General may bring an action to address violations of this section. The Office of the Attorney General may impose a civil penalty **not to exceed \$150,000 per breach of the security of the system** or a series of breaches of a similar nature that are discovered in a single investigation. Nothing in this section shall limit an individual from recovering direct economic damages from a violation of this section.

What information is protected?

“Medical information” means the following:

- Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
- An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

Notification of Breach

If **unencrypted or unredacted** medical information **was or is reasonably believed to have been accessed** and acquired by an unauthorized person, an entity⁸⁵ that owns or licenses computerized data that includes medical information **shall disclose** any breach of the security of the system⁸⁶ **following discovery or notification** of the breach of the security of the system **to the Office of the Attorney General, the Commissioner of Health, the subject of the medical information, and any affected resident of the Commonwealth without unreasonable delay.**

An entity **shall disclose** the breach of the security of the system if **encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key.**

Notice required by this section **may be reasonably delayed** to allow the entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system.

Notice required by this section **may be delayed** if, after the entity notifies a law-enforcement agency, the law-enforcement agency determines and advises the entity that the notice will impede a criminal or civil investigation, or homeland or national security.

⁸⁵ “Entity” means any authority, board, bureau, commission, district or agency of the Commonwealth or of any political subdivision of the Commonwealth, including cities, towns and counties, municipal councils, governing bodies of counties, school boards and planning commissions; boards of visitors of public institutions of higher education; and other organizations, corporations, or agencies in the Commonwealth supported wholly or principally by public funds.

⁸⁶ Breach of the security of the system” means **unauthorized access and acquisition of unencrypted and unredacted** computerized data that compromises the security, confidentiality, or integrity of medical information maintained by an entity.

Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

Third Party: An entity that maintains computerized data that includes medical information that the entity **does not own** or license **shall notify** the owner or licensee of the information of any breach of the security of the system **without unreasonable delay following discovery of the breach of the security of the system**, if the medical information **was accessed and acquired** by an unauthorized person **or the entity reasonably believes the medical information was accessed and acquired** by an unauthorized person.

Requirements for Notification

Notice required by this section shall include a description of the following:

- The incident in general terms;
- The type of personal information that was subject to the unauthorized access and acquisition;
- The general acts of the individual or entity to protect the personal information from further unauthorized access;
- A telephone number that the individual may call for further information and assistance, if one exists; and

Notice means any of the following:

- Written notice to the last known postal address in the records of the individual or entity;
- Telephone notice;
- Electronic notice; or
- Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed **\$50,000**, the affected class of Virginia residents to be notified exceeds **100,000** residents, or the individual or the entity does not have sufficient contact information or consent to provide notice as described above. Substitute notice consists of all of the following:
 - Email notice if the individual or the entity has email addresses for the members of the affected class of residents;

- Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and

Notice to major statewide media.

In the event an entity provides notice to **more than 1,000 persons** at one time, pursuant to this section, the entity **shall notify**, without unreasonable delay, **the Office of the Attorney General and the Commissioner of Health of the timing, distribution, and content of the notice.**

Penalty

No listed penalty.

51. Washington

Wash. Rev. Code Ann. §§ 19.255.010 (2005)

What information is protected?

“Personal information” means the following:

- An individual’s first name or first initial and last name in combination with any one or more of the following data elements:
 - Social security number;
 - Driver’s license number or Washington identification number; or
 - Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

Notification of Breach

Any person or business that conducts business in this state and that owns or licenses data that includes personal information **shall disclose** any breach of the security of the system⁸⁷ **following discovery or notification** of the breach in the security of the data to any resident of this state whose personal information **was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured (safe harbor).**⁸⁸

⁸⁷ “Breach of the security of the system” means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.

⁸⁸ “Secured” means encrypted in a manner that meets or exceeds the national institute of standards and technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person.

Notice is not required if the breach of the security of the system is **not reasonably likely to subject consumers to a risk of harm.**

The **breach of secured personal** information **must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person.**

Notification to affected consumers and to the attorney general under this section **must be made in the most expedient time possible and without unreasonable delay, no more than forty-five** calendar days after the breach was discovered, unless at the request of law enforcement as, or due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Third Party: Any person or business that maintains data that includes personal information that the person or business **does not own shall notify** the owner or licensee of the information of any breach of the security of the data **immediately following discovery**, if the personal information **was, or is reasonably believed to have been,** acquired by an unauthorized person.

The notification required by this section **may be delayed** if the data owner or licensee contacts a law enforcement agency after discovery of a breach of the security of the system and a law enforcement agency determines that **the notification will impede a criminal investigation.** The **notification** required by this section **shall be made after** the law enforcement agency determines that **it will not compromise the investigation.**

Requirements for Notification

Any person or business that is required to issue notification shall meet all of the following requirements:

- The notification must be written in plain language; and
- The notification must include at a minimum, the following information:
 - The name and contact information of the reporting person or business subject to this section;

- A list of the types of personal information that were or are reasonably believed to have been the subject of a breach; and
- The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.

Notice may be provided by one of the following methods:

- Written notice;
- Electronic notice, if consistent with 15 U.S.C. 7001; or
- Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed **two hundred fifty thousand dollars**, or that the affected class of subject persons to be notified exceeds **five hundred thousand**, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:
 - Email notice when the person or business has an email address for the subject persons;
 - Conspicuous posting of the notice on the website page of the person or business, if the person or business maintains one; and
 - Notification to major statewide media.

Any person or business that is required to issue a notification pursuant to this section to **more than five hundred Washington residents** as a result of a **single breach** shall, by the time notice is provided to affected consumers, **electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the attorney general**. The person or business shall **also provide to the attorney general the number of Washington consumers affected by the breach, or an estimate** if the exact number is not known.

Penalty

Any consumer injured by a violation of this section may institute a civil action to recover damages.

Any consumer injured by a violation of this section may institute a civil action to recover damages.

The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

52. West Virginia

W. Va. Code Ann. §§ 46A-2A-101 (2008)

What information is protected?

“Personal information” means the following:

- The first name or first initial and last name linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are **neither encrypted nor redacted**:
 - Social security number;
 - Driver’s license number or state identification card number issued in lieu of a driver’s license; or
 - Financial account number, or credit card, or debit card number in combination with any required security code, access code or password that would permit access to a resident’s financial accounts.

Notification of Breach

An individual or entity that owns or licenses computerized data that includes personal information **shall give notice** of any breach of the security of the system⁸⁹ **following discovery or notification** of the breach of the security of the system to any resident of this state whose unencrypted **and unredacted personal information was or is reasonably believed to have been accessed and acquired** by an unauthorized person and that causes, or the individual **or entity reasonably believes has caused or will cause**, identity theft or other fraud to any resident of this state.

The notice shall be made **without unreasonable delay**, unless delayed by a law enforcement agency because notice will impede a criminal or civil investigation or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the notice shall be made without unreasonable delay.

An individual or entity **must give notice** of the breach of the security of the system **if encrypted information is accessed and acquired in an unencrypted form or if the security breach involves a person with access to the encryption key** and the individual or entity **reasonably believes that such breach has caused or will cause identity theft or other fraud** to any resident of this state.

⁸⁹ “Breach of the security of a system” means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident of this state.

Third Party: An individual or entity that maintains computerized data that includes personal information that the individual or entity **does not own** or license **shall give notice** to the owner or licensee of the information of any breach of the security of the system **as soon as practicable following discovery**, if the personal information **was or the entity reasonably believes was accessed and acquired** by an unauthorized person

Requirements for Notification

The notice shall include:

- To the extent possible, a description of the categories of information that were reasonably believed to have been accessed or acquired by an unauthorized person, including social security numbers, driver's licenses or state identification numbers and financial data;
- A telephone number or website address that the individual may use to contact the entity or the agent of the entity and from whom the individual may learn:
 - What types of information the entity maintained about the individual or about individuals in general; and
 - Whether or not the entity maintained information about the individual;
- The toll-free contact telephone numbers and addresses for the major credit reporting agencies and information on how to place a fraud alert or security freeze.

A person may give notice by providing:

- Written notice to the postal address in the records of the individual or entity;
- Telephonic notice;
- Electronic notice, if consistent with 15 U.S.C. 7001;
- Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed **fifty thousand dollars** or that the affected class of residents to be notified exceeds **one hundred thousand persons** or that the individual or the entity does not have sufficient contact information or to provide notice. Substitute notice consists of any **two** of the following:
 - Email notice if the individual or the entity has email addresses for the members of the affected class of residents;

- Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; or
- Notice to major statewide media.

If an entity is required to notify **more than one thousand persons** of a breach of security pursuant to this article, the entity **shall also notify, without unreasonable delay, all consumer reporting agencies** that compile and maintain files on a nationwide basis of the timing, distribution and content of the notices.

Penalty

Failure to comply constitutes an unfair or deceptive act or practice, which may be enforced by the attorney general. The attorney general shall have exclusive authority to bring action. No civil penalty may be assessed in an action unless the court finds that the defendant has engaged in a course of repeated and willful violations. No civil penalty shall exceed \$150,000 per breach of security of the system or series of breaches of a similar nature that are discovered in a single investigation.

53. Wisconsin

Wis. Stat. Ann. § 134.98 (2006), as amended (2008)

What information is protected?

“Personal information” means the following:

- An individual’s last name and the individual’s first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is **not encrypted, redacted, or altered in a manner that renders the element unreadable:**
 - The individual’s social security number;
 - The individual’s driver’s license number or state identification number;
 - The number of individual’s financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual’s financial account;
 - The individual’s deoxyribonucleic acid profile;
 - The individual’s unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

Notification of Breach

If an entity whose principal place of business **is located in this state** or an entity that maintains or licenses personal information in this state **knows that personal information in the entity’s possession has been acquired** by a person whom the entity has not authorized to acquire the

personal information, the entity **shall make reasonable efforts to notify each subject of the personal information.**

If an entity whose principal place of business **is not located in this state knows that personal information pertaining to a resident of this state has been acquired by a person whom the entity has not authorized to acquire** the personal information, the entity **shall make reasonable efforts to notify each resident of this state who is the subject of the personal information.**

An entity shall provide the notice required **within a reasonable time, not to exceed 45 days after the entity learns of the acquisition** of personal information. A determination as to reasonableness under this paragraph shall include consideration of the number of notices that an entity must provide and the methods of communication available to the entity.

An entity is **not required to provide notice** of the acquisition of personal information if the acquisition of personal information **does not create a material risk of identity theft or fraud** to the subject of the personal information.

Third Party: If a person, other than an individual, that stores personal information pertaining to a resident of this state, **but does not own or license** the personal information, **knows that the personal information has been acquired** by a person whom the person storing the personal information has not authorized to acquire the personal information, and the person storing the personal information has not entered into a contract with the person that owns or licenses the personal information, the person storing the personal information **shall notify the person that owns or licenses the personal information of the acquisition as soon as practicable.**

Law Enforcement: A law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to provide a notice for any period of time and the notification process required shall begin at the end of that time period. If an entity receives such a request, the entity may not provide notice of or publicize an unauthorized acquisition of personal information, except as authorized by the law enforcement agency that made the request.

Requirements for Notification

The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information.

An entity shall provide the notice required under by:

- Mail; or
- By a method the entity has previously employed to communicate with the subject of the personal information.

If an entity cannot with reasonable diligence determine the mailing address of the subject of the personal information, and if the entity has not previously communicated with the subject of the personal information, the entity shall provide notice by a **method reasonably calculated to**

provide actual notice to the subject of the personal information.

Upon written request by a person who has received a notice, the entity that provided the notice shall identify the personal information that was acquired.

If, as the result of a single incident, an entity is required to notify **1,000 or more** individuals that personal information pertaining to the individuals has been acquired, the entity shall **without unreasonable delay notify all consumer reporting agencies** that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices sent to the individuals.

Penalty

Failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or breach of a legal duty.

54. Wyoming

Wyo. Stat. Ann. § 40-12-501 (2015)

What information is protected?

“Personal information” means the following:

- The first name or first initial and last name of a person in combination with one or more of the following data elements when either the name or the data elements **are not redacted**⁹⁰:
 - Social security number;
 - Driver’s license number or Wyoming identification card number;
 - Account number, credit card number or debit card number in combination with any security code, access code or password that would allow access to a financial account of the person;
 - Tribal identification card;
 - Federal or state government issued identification card;
 - Username or email address, in combination with a password or security question and answer that would permit access to an online account;
 - Birth or marriage certificate;

⁹⁰ “Redact” means alteration or truncation of data such that no more than five digits of the data elements provided are accessible as part of the personal information.

- Medical information, meaning a person’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;
- Health insurance information, meaning a person’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the person or information related to a person’s application and claims history;
- Unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes; or
- Individual taxpayer identification number.

Notification of Breach

An individual or commercial entity that conducts business in Wyoming and that owns or licenses computerized data that includes personal identifying information about a resident of Wyoming **shall, when it becomes aware of a breach of the security of the system,⁹¹ conduct in good faith a reasonable and prompt investigation** to determine the likelihood that personal identifying information has been or will be misused.

If the investigation determines that the misuse of personal identifying information about a Wyoming resident **has occurred or is reasonably likely to occur**, the individual or the commercial entity **shall give notice as soon as possible to the affected Wyoming resident**.

Notice shall be made in the **most expedient time possible and without unreasonable delay**, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

Third Party: Any person who maintains computerized data that includes personal identifying information **on behalf of another business** entity **shall disclose** to the business entity for which the information is maintained any breach of the security of the system **as soon as practicable following the determination that personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person**.

The person who maintains the data on behalf of another business entity and the business entity on whose behalf the data is maintained may agree which person or entity will provide any required notice, provided only a single notice for each breach of the security of the system shall be required. If agreement regarding notification cannot be reached, the person who has the direct business relationship with the resident of this state shall provide notice.

Requirements for Notification

⁹¹ “Breach of the security of the data system” means unauthorized acquisition of computerized data that **materially compromises** the security, confidentiality or integrity of personal identifying information maintained by a person or business and causes or is reasonably believed to cause loss or injury to a resident of this state.

Notice required of this section shall be clear and conspicuous and shall include, at a minimum:

- A toll-free number:
 - That the individual may use to contact the person collecting the data, or his agent; and
 - From which the individual may learn the toll-free contact telephone numbers and addresses for the major credit reporting agencies;
- The types of personal identifying information that were or are reasonably believed to have been the subject of the breach;
- A general description of the breach incident;
- The approximate date of the breach of security, if that information is reasonably possible to determine at the time notice is provided;
- In general terms, the actions taken by the individual or commercial entity to protect the system containing the personal identifying information from further breaches;
- Advice that directs the person to remain vigilant by reviewing account statements and monitoring credit reports;
- Whether notification was delayed as a result of a law enforcement investigation, if that information is reasonably possible to determine at the time the notice is provided.

Notice to consumers may be provided by one of the following methods:

- Written notice;
- Electronic mail notice;
- Substitute notice, if the person demonstrates that
 - The cost of providing notice would exceed **ten thousand dollars** for Wyoming-based persons or businesses, and **two hundred fifty thousand dollars** for all other businesses operating but not based in Wyoming;
 - That the affected class of subject persons to be notified exceeds **ten thousand** for Wyoming-based persons or businesses and **five hundred thousand** for all other businesses operating but not based in Wyoming; or
 - The person does not have sufficient contact information.
 - Substitute notice shall consist of all of the following:
 - Conspicuous posting of the notice on the Internet, the World Wide Web or similar proprietary or common carrier electronic system site of the person

collecting the data, if the person maintains a public Internet, the World Wide Web or a similar proprietary or common carrier electronic system; and

- Notification to major statewide media. The notice to media shall include a toll-free phone number where an individual can learn whether or not that individual's personal data is included in the security breach.

Penalty

The attorney general may bring an action in law or equity to address any violation of this section and for other relief that may be appropriate to ensure proper compliance with this section, to recover damages, or both. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law.

II. Europe

1. EU's General Data Protection Regulation ("GDPR")

General Data Protection Regulation (GDPR) 2016/679, OJ L'119/1-88 (EU)

(1) Beginning May 25, 2018

In every instance where a company either collects or holds any personal data of a person or data subject in the European Union⁹², a company must obtain EXPRESS WRITTEN CONSENT from that person so long as the data is not de-identified. To the extent the person can be discerned from the data, for example, data from clinical trials, demos, etc., a company needs express consent. **If the data is de-identified, then no consent is needed. If the data is from a country not part of the EU, then GDPR does not apply.**

Data includes:

- **any information relating to an identified or identifiable natural person**
- **identifiable data types (including, but not limited, to):**
 - **name**
 - **address**
 - **phone number**
 - **email address**
 - **financial accounts**
 - **Medical information:** *Both GDPR and HIPAA address privacy and security of medical records. The overlap in the regulations exists for "data concerning health," which the GDPR defines as any personal data relating to the physical or mental health of an individual, including any health care service which may reveal information about the person's health status.*

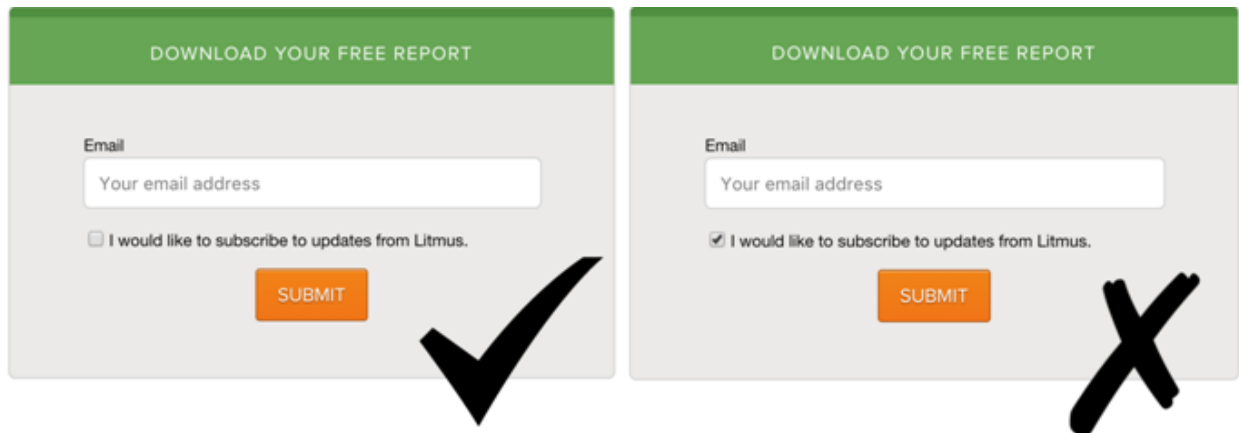
⁹² Primary Countries that will be affected: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom (regardless of Brexit, UK is still implementing GDPR and will likely remain subject to, or implement a law functionally similar).

- identification number
- location data
- online identifier (i.e. cookies- when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them, IP address, RFID tags)
- biometric data
- racial/ethnic data
- sexual orientation
- political opinions
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person

All data collected through the above list will be subject to GDPR and requires Express WRITTEN Consent to collect, store, and process that data.

EXPRESS CONSENT can be obtained by utilizing a Consent Form. All requests by a company for consent to collect and use the data must be given in an intelligible manner with clear and plain language, and should be separate from other consents.

OPT-IN vs. OPT-OUT: GDPR specifies that express consent requires each person to “Opt-in.” Opting in requires an affirmative action. **Default consent WILL NOT work**, and, companies must make it as easy to opt-out as it is to opt-in. Opting out should be as simple as finding the same form that was used to opt-in. **All forums where a company collects any data, including online forums, text messaging, social media, apps, etc., require an affirmative action by the person to have his or her data collected and processed.** For consent to be valid, a customer must actively confirm consent, such as clicking an **unchecked** opt-in box, and opting out must be as simple as un-clicking that opt-in box. **Pre-checked boxes will not work.** Here is an example:



EXPRESS CONSENT REQUIRES DISCLOSING ALL PURPOSES FOR THE COLLECTION AND PROCESSING OF THE DATA. IF THAT PURPOSE CHANGES, NEW CONSENT MUST BE OBTAINED.

In order to give express consent, or if consent is for the collection and processing of data for multiple purposes, the consent must set forth all purposes in which that person is giving consent. **(For example: Signing up for an email list for advertising purposes, and signing up to view a webinar- two purposes, and both purposes for a company’s collection of their data must be clearly set forth when consent is**

given.)

Storing Data: Companies must store all personal data collected in a highly secure manner for only as long as necessary based on the purpose for which the data is processed. If at all possible, companies should store “pseudonymized” data, which makes connecting the data to the individual almost impossible. Pseudonymized data is less rigorously guarded, and therefore, there is an incentive to store as much information in this format as possible.

Consent Form: The form must set out the purposes and lawful bases for all processing activities, the data retention period, information concerning the rights of the data subject (specifically, how to opt-out), and the right to complain to a data protection authority. The purpose section must be unambiguous.

(2) Appointing a Data Protection Officer (“DPO”)

Some organizations are required to appoint data protection officers to oversee their ongoing data collection and processing. The Controller and Processor (roles discussed below) must designate a data protection officer in any case where the processing is being carried out by a public authority (excluding courts), the core activities of the controller or the processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale, or processing **special categories** of personal data on a large scale pursuant to Art. 9. **Controllers or processors outside the EU are required to appoint a representative in the EU as a point of contact for data subjects and supervisory authorities unless the processing is occasional, and does not involve large scale processing of sensitive personal data.**

Data collected by certain companies may aggravate some of the special categories, for example:

Special categories of data listed under Art. 9 include processing of personal data revealing **racial or ethnic origin**, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of **genetic data**, biometric data for the purpose of uniquely identifying a natural person, **data concerning health or data concerning a natural person’s sex life** or sexual orientation.

The DPO can be the same person as the Chief Information Security Officer.

Appointment of a DPO is necessary if a company collects data concerning health. When appointing the DPO, the DPO will be responsible for ongoing review, monitoring compliance, advising employees and communicating with the supervising authority in the event a company is questioned or reporting in response to a data breach is necessary.

(3) Appointment of Controller and Processor

A **Controller** means the natural or legal person(s) who alone or jointly with others, determines the purposes and means of the processing of personal data.

A **Processor** means a natural or legal person or other body which processes personal data on behalf of the Controller. The Processor is the data management company or other organization that stores/digitizes the information.

(4) Agreements and Terms and Conditions

All healthcare provider facing documents involving collection of any data listed in Section 1 must be updated to comply with GDPR. If any of the data listed in Section 1 is collected and stored, a company

must obtain consent. Consent must be separate from the terms and conditions and/or the Agreement, as GDPR requires the consent to be distinguishable from consent to other matters provided in related Agreements

New consent can be obtained by sending emails to existing customers in the company’s databases and from anyone in which a company holds data, and inform them of the changes (or creation of) terms and conditions for the usage of their data. The message can be:

(5) Communications

A. Emails/Texts: All mailing lists, created before or after May 25, 2018, will require EU users’ consent to receive continued emailing/texts and must disclose what data and why that data is being collected. Do not send emails or text messages without consent. Once the relationship is established, and consent has been received, emails and texts are appropriate as long as they are within the scope of the consent that was given. Consent to one type of communication on one topic is not all encompassing.

B. Websites:

a. **Privacy Policy:** A company must update the language in the policy section to address compliance with GDPR.

b. **Collecting Cookies:** Requires consent. Add a phrase to the privacy policy that states (and requires an affirmative opt-in) :

We use Cookies. If you're happy with cookies, continue browsing.

PROCEED

c. **Consent from Children under the age of 18:** This compendium presumes that a company does not collect data from children. But to the extent, a company does collect such data, then the company must add a phrase to the website that states, “**We do not collect any information from anyone under 18 years of age. Our website is directed to persons who are at least 18 years of age or older and medical professionals.**”

(6) Maintaining Records of Consent

A. Internal Documentation System: GDPR requires companies to keep evidence of who consents, when, and how for all forums where the company collects data. The company must be able to provide proof of who consented, when they consented, what they were told at the time of consent, how they consented, and whether they have withdrawn consent.

B. Email Subscribers: A company must audit current email lists and determine whether the above questions can be answered (i.e., whether they have provided GDPR-proof consent), and if not, new consent is needed.

C. Unsubscribe

a. A company must provide a mechanism for unsubscribing.

(7) Data Retention

- A. **Data Security:** All data collected and processed must be stored in a highly secure manner. The data must also be easily accessible and easy to remove from any lists/databases maintained, as individuals must be able to delete or request that their data be deleted completely. A data subject has the right to ask the Controller about his/her data collected such as:
- a. The purpose of the processing;
 - b. The categories of personal data concerned;
 - c. The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
 - d. Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 - e. The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
 - f. The right to lodge a complaint with a supervisory authority;
 - g. Where the personal data are not collected from the data subject, any available information as to their source;
 - h. The existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- B. **Right to be forgotten:** Data subjects have the right to request that the Controller erase all personal data without undue delay. This could be due to withdrawn consent or the personal data is no longer necessary in connection with the purpose it was initially collected. **A company will have 30 days to erase the data.**
- C. **Third-Party Data Processors:** Additional care must be taken when selecting third-party providers that access and process personal data for a company, including cloud service providers. GDPR places the burden of proof on the Controller. If the company utilizes a data processor, that data processor must be GDPR compliant, and therefore, a company must update any third-party contracts (Think: distributor agreements) with addenda that include an indemnification provision in the instance that the service provider is sued for a violation of GDPR.
- D. **Data Retention:** Data should only be retained for however long is reasonably necessary.

(8) Data Breach Policy

In the case of a personal data breach, the company **has 72 hours after becoming aware of the breach to notify the supervising authority of same in accordance with Art. 55, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Failure to report within 72 hours will require an explanation for delay.** If the breach is likely to result in a high risk to the rights of individuals affected by the breach, those affected must be notified directly.

Notification of a breach will need to include:

1. A description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

2. Communication of the name and contact details of the data protection officer or other contact point where more information can be obtained;
3. A description of the likely consequences of the personal data breach;
4. A description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Reporting to the Supervising Authority: If the company is located outside of the EU, it will be difficult to determine the location of its “main establishment.” A company’s “main establishment” in theory would be the location where a company carries out the most data processing which substantially affects individuals in other EU member states. The location of the main establishment determines the Lead Supervising Authority (“LSA”). In the event of a breach, companies are required to notify the lead supervising authority. If the company cannot determine a location for the “main establishment” then the company will be exposed to supervising authorities in various EU member states. This could mean potentially having to report a breach to multiple supervising authorities.

Although GDPR does not set forth sanctions for entities that fail to appoint a LSA, it is unclear if the failure to appoint a LSA will cause a supervising authority to question a company understanding of the GDPR in other areas. Therefore, if a company can establish a central administration location, this will assist in being able to appoint a LSA.

In cases where a company’s main establishment is located outside of the EU, in order to determine the location of the LSA, that company must consider:

- Where are decisions relating to purposes and means of processing given final “sign-off”?
- Where are decisions about business activities that involve data processing made?
- Where does the power to have decisions implemented effectively lie?
- Where is the director (or directors) with overall management responsibility for the cross-border processing located?
- Where is the controller or processor registered as a company, if in a single territory?

(9) Cross-Border Data Transfers

Personal data cannot be transferred outside of the EU unless the GDPR’s requirements are met to a country the European Commission has determined provides an adequate level of protection to personal data. The United States does not qualify; however, transfers are permitted under the EU-U.S. privacy shield regime, which involves a self-certification process for U.S. organizations.

Self-Certification: The EU-US privacy certification provides companies on both sides of the Atlantic the ability to comply with data transfer laws. The Privacy Shield Program administered by the U.S. Department of Commerce enables U.S. companies to join a Privacy Shield Framework where a company would publicly commit to comply with the privacy shield principles which include notice to individuals, offer the choice to opt-out, accountability of onward transfer, security, data integrity and purpose limitation, individuals must have access to their own personal information, recourse/enforcement/liability, and supplemental principles.

In order to become eligible, companies must develop a privacy shield compliant policy statement, identify an independent resource mechanism, pay a required fee to the ICDR-AAA (binding arbitration), ensure a

verification mechanism is in place, designate a contact, and submit a self-certification to the Department of Commerce. Overall, the privacy shield mirrors that of GDPR.

(10) Fines

Under GDPR, a company could be exposed to various fines for failing to comply. Each member state may individually invoke a fine, in addition to administrative fines. A company can be fined up to 4% of annual global turnover or 20 million euro, whichever is greater, for breach of the GDPR. This maximum fine is only for the most serious infringements, i.e., not having sufficient customer consent to process data.

European Data Protection Board Guidelines – Territorial Scope of GDPR

On November 23, 2018, the European Data Protection Board (“EDPB”) issued guidelines on the territorial scope of the GDPR. The guidelines are perhaps most important for companies located outside the E.U. seeking to understand the GDPR’s application to their respective business activities. Generally speaking, the guidelines focus on two principles that define the GDPR’s territorial scope: (1) the “establishment” criterion (Article 3(1)) and (2) the “targeting” criterion (Article 3(2)).

The EDPB defined the establishment criterion as any real or effective activity exercised through “stable arrangements.” The EDPB specified that an establishment may be a formal arrangement such as a subsidiary or branch, but may also include “the presence of one single employee or agent . . . if that employee or agent acts with a sufficient degree of stability.”

The EDPB also expounded on the targeting criterion, and clarified that the GDPR’s reference to data subjects in the EU does not require a data subject to have citizenship or residency status in same. In addition, the EDPB clarifies that for the GDPR to apply, the conduct of the controller or processor must indicate the *intent* to offer goods and service to individuals in the EU. Factors to consider include:

- Delivery of goods in European Union Member States;
- The use of European Union Member State language or currency;
- Dedicated addresses or phone numbers for the company to be reached from the European Union;
- The international nature of the activity;
- Marketing and advertisements directed at individuals in the European Union; and
- The use of a European Union Member State top-level domain name (e.g., .eu).

When viewed collectively, the factors highlighted in the guidelines may provide evidence of “an intention to establish commercial relations” sufficient to trigger extraterritorial application of the GDPR.

2. ePrivacy Regulation

EU’s NEW ePrivacy Regulation- replaces the ePrivacy directive from 2002

The new regulation specifically protects the confidentiality of electronic communications. The current draft is still under review, but if it prevails, websites that allow interactions must obtain

explicit consent before placing any tracker codes on users' devices or collecting data about their communications- ***Although your company does not use online messaging, etc., you will likely be impacted by the browser setting/collection of cookies on its website and any online marketing.***

Interestingly, the ePrivacy Regulation is self-executing and will be binding across the EU, whereas the directive it is replacing (and much like the GDPR directive), required local regulations for implementation with the consequence of inconsistent enforcement. Also, for some history, the initial e-Privacy Directive from 2002 was a complement of the EU's initial Data Protection Directive, which was replaced by GDPR. Therefore, the ePrivacy regulation is intended to complement the GDPR and strive towards uniformity across the market.

The ePrivacy directive was initially known as the "cookie law"- the new version will include more forms of data in addition to traditional telecommunications, such as all digital communications including but not limited to texting and video chat apps. The scope of the new law applies to any business that provides any form of online communication service (WhatsApp, Facebook Messenger, Skype), uses online tracking technologies, or engages in electronic direct marketing. Metadata must have a high privacy component and must be anonymized or deleted if users did not give their consent unless needed for billing purposes. There will be one condition under which a company may use data or metadata about users' electronic communications: obtaining consumers' explicit and informed consent for the agreed-upon purpose.

The ePrivacy Regulation aims to simplify the rules regarding cookies and streamline cookie consent in a more 'user-friendly' way. This will remove the overload of consent requests and streamline consent through browser settings.

When will it go into effect?

The date the ePrivacy regulation will be published or go into effect is not clear (it is expected 2019) however the amended proposed text was approved by the plenary of the EU parliament at the end of October 2017.

Penalties

Penalties for noncompliance are up to 20 million euro.

Some changes to come:

- Browser settings will enable website visitors to accept or refuse cookies as well as other identifiers.
- Consent may not be needed for "non-privacy intrusive cookies."
- There will be a ban from unsolicited electronic communications.

Enforcement

Enforcement of these rules will be the responsibility of the same data protection authorities already overseeing GDPR.

3. "The Right to Be Forgotten"

On May 13, 2014, The Court of Justice of the European Union (hereinafter the "CJEU")

established a data subject's "right to be forgotten." The CJEU found that data processors, *e.g.* Google, could be forced to remove personal information that is "inadequate, irrelevant . . . or excessive in relation to the purpose for which they were processed and in the light of the time that has elapsed" upon request of the data subject. The Court's ruling, however, never defined how, when, and where data processors should remove the personal information.

Following the CJEU's decision, Google responded to many requests for delisting of information; however, delisting was only carried out on the European extensions of the search engine. On June 12, 2015, The Commission Nationale de L'informatique et des Libertés of France (**hereinafter the "CNIL"**) responded by issuing a public notice opining on Google's haphazard observance to the CJEU's decision. The CNIL noted that, "in order to be effective, delisting must be carried out on *all extensions of the search engine* and that service provided by Google search constitutes a single processing." In other words, the CNIL interprets the CJEU decision to apply to search engine results globally, not just within the European Union.

On September 11, 2018, the CJEU heard oral arguments on whether the "right to be forgotten" can and should stretch beyond the borders of the European Union. Google urged that extending the right beyond the European Union was "completely unenvisagable," and such a step would "unreasonably interfere" with people's freedom of expression. By contrast, the CNIL believes limiting the "right to be forgotten" to the European Union would amount to "dead rights." An advisory opinion is scheduled to be delivered on December 11, 2018.

4. EU-US Privacy Shield

Self-Certification: The EU-US privacy certification provides companies on both sides of the Atlantic the ability to comply with data transfer laws. The Privacy Shield Program administered by the U.S. Department of Commerce enables U.S. companies to join a Privacy Shield Framework where they would publicly commit to comply with the privacy shield principles which include notice to individuals, offer the choice to opt-out, accountability of onward transfer, security, data integrity and purpose limitation, individuals must have access to their own personal information, recourse/enforcement/liability, and supplemental principles.

In order to become eligible, a company must develop a privacy shield compliant policy statement, identify an independent resource mechanism, pay a required fee to the ICDR-AAA (binding arbitration), ensure a verification mechanism is in place, designate a contact, and submit a self-certification to the Department of Commerce. Overall, the privacy shield mirrors that of GDPR.

On July 26, 2018, the European Parliament issued a resolution on the adequacy of the protection afforded by the EU-US Privacy Shield, which called for its suspension if the U.S. failed to fully comply with the agreement's terms and conditions by September 1, 2018.

The deadline has since come and gone, and the U.S. made no effort to comply with the resolution. Since the deadline, no suspension has been announced and the European Commission has yet to make any public statement. Should the Privacy Shield be suspended, however, the self-reporting attestation abilities of companies doing business with EU citizens would be

limited. Therefore, all companies attempting to do business in the EU would come under the GDPR compliance scope.

III. Angola

Angolan Data Protection Act, Law No. 22/11 (2011)

Personal Information

Angola's Data Protection Law ("DPL") defines personal information as any given information, regardless of its nature, including images and sounds related to a specific individual. Sensitive personal information means personal information related to:

- Philosophical or political beliefs;
- Political affiliation/trade union membership;
- Religion;
- Private life;
- Racial or ethnic origin;
- Health or sex life (including genetic data).

Registration and Protection Authority

The Agencia de Protecao de Dados (ADP) is tasked with enforcing the DPL, although it has not been established yet.

Prior to processing personal information, the company must either:

- Prior notification to APD; or
- Prior authorization from the APD.

Notification and authorization request should include the following information:

- The name and address of the controller and its representative;
- The purpose of the processing;
- A description of the data;
- The recipients to whom the personal information may be communicated;
- Details of any third party responsible for processing;

- The possible combinations of personal data;
- The duration of retention;
- The process and conditions of right of access, rectification, deletion, opposition, and updating;
- Any predicted transfers to third countries;
- A general description.

Data Protection Officers

No obligation on the company.

Collection and Processing

Under the DPL, person data collection and processing is subject to express and prior consent from the individual, as well as prior notification to the APD. Prior authorization from the APD is required to obtain sensitive personal information.

A company must adhere to the following principles regarding the collection and processing of personal information: transparency, legality, good faith, proportionality, truthfulness, and respect to private life as well as to the legal and constitutional guarantees. Data processing shall also be limited to the purpose for which the data is collected, and personal information shall not be held longer than is necessary for that purpose.

Transfer of Personal Information

Transfer to countries with an adequate level of protection require prior notification to the APD. The APD issues opinions regarding the adequacy of a countries level of protection. If a country does not have an adequate level of protection, the APD may give authorization, which will only be granted on a case-by-case basis.

Security of Personal Information

A company must implement appropriate technical and organizational measures to protect personal information from destruction, loss, alteration, unauthorized disclosure, and against unlawful forms of processing.

Breach Notification

There is no breach notification requirement under the DPL.

Enforcement

The competent authority for the enforcement of the DPL is not yet created; thus, the level of enforcement is not significant at this time.

IV. Argentina

Law No. 25326, Oct. 30, 2000, [X] B.O. 30 (Arg.)

In October 2000, Argentina enacted the Personal Data Protection Law Number 25,326 (“PDPL”).

Personal Information

The PDPL defines personal information as “any type of information related to identify or identifiable individuals or legal entities.” Sensitive information means “personal information revealing racial or ethnic origin, political views, religious beliefs, philosophical or moral stands, union affiliations or any information referring to health or sexual life.”

Registration

A private or public data file, register, base or bank intended to provide reports must be registered with the Direccion Nacional de Proteccion de Datos Personales (DNPDP). The registration must include the following:

- Name and address of the data collector;
- Characteristics and purpose of the database;
- Nature of the data included in the database;
- Collection and update methods;
- Individuals or entities to which the data may be transferred;
- Methods for linking the recorded information;
- \methods used to ensure data security, including a detail of the people with access to information processing;
- Time during which the data will be stored; and
- Conditions under which third parties can gain access and the procedures performed to correct or update the data.

Data Protection Officers

Not required. However, a “Head of Data Security” must be appointed by companies to which “medium” or “high” security requirements apply.

Collection & Processing of Personal Information

Generally speaking, a company may only collect and process personal data with the data subject's consent. However, consent is **not** required if:

- The personal information is collected from a public accessible database, in the exercise of government duties, or as a result of a legal obligation;
- The database is limited to certain basic information;
- The information derives from a scientific or professional contractual relationship and used in that context.

When collecting personal information, the company shall expressly and clearly inform the individuals of:

- The purpose;
- Who may receive the information;
- The existence of a database;
- The identity of the company collecting the information and its mailing address;
- The consequences of refusal or of providing inaccurate information; and
- The rights of access, rectification, and suppression by the individual.

The collection of personal information must be truthful, adequate, pertinent, and not excessive, be used exclusively for the purpose for which it was legally obtained, and deleted upon completion of that purpose.

No person may be required to disclose sensitive personal information, and it may only be collected and processed in cases of public interest, as determined by law. Additionally, information related to criminal history or background may **only** be collected by public authorities.

Transfer

Personal data may only be transferred outside of Argentina in compliance with legitimate interests of the transferring and receiving parties, and generally requires consent by the individual, which may later be revoked. Consent is **not required** when:

- The collection of the data did not require consent;
- The data relates to health issues, and is used for emergencies, epidemiologic studies or other public health purposes, provided that the identity of the subject is protected;
- The information has been de-identified such that they may no longer be linked with the corresponding subject.

Both parties of the transfer are jointly and severally liable for any breach of data obligations.

Personal data may not be transferred to a country that does not provide adequate levels of protection.

Security of Personal Information

A company must take all technical and organizational measures necessary to ensure the security and confidentiality of the personal information, so as to avoid alteration, loss, or unauthorized access or treatment. The level of security that must be provided varies in relation to the sensitivity of the personal data.

Breach Notification

Not required. All breaches must be recorded by the company in a “security incidents ledger,” which is accessible to the DNPDP when conducting inspections.

Enforcement

Sanctions include warnings, suspensions, the imposition of monetary fines ranging from AR\$1,000 to AR\$100,000, or the cancellation of the database. In addition, individuals may separately recover damages in violation of their data protection rights.

V. Australia

Federal Privacy Act, 1988 (Cth) ss 1-83 (Austl.)

Personal information protection in Australia is a mix of Federal and State/Territory legislation. The Federal Privacy Act 1988 (“PA”) and its Australian Privacy Principles (“APP”) apply to private companies with an annual turnover of at least A\$3 million.

Personal Information

“Personal information” means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in material form or not. Sensitive personal information means information or an opinion about:

- Health;
- Racial or ethnic origin;
- Political opinions;
- Membership of a political association, professional or trade association or trade union;
- Religious belief or affiliations;

- Philosophical beliefs;
- Sexual orientation and practices;
- Criminal record;
- Biometric information that is to be used for certain purposes;
- Biometric templates.

Data Protection Officers

No required, but good and usual practice under the law and guidance has been issued by the Privacy Commissioner that strongly recommends it.

Collection & Processing of Personal Information

The collection of personal information must be reasonably necessary for one or more of a company's business functions or activities. Under the PA, the company must take steps, as are reasonable in the circumstances, to ensure that the personal information is accurate, up-to-date, and correct.

At or before the time the information is collected, a company must take reasonable steps to make an individual aware of the following:

- The company and its contact information;
- The purpose;
- To whom the information may be given;
- Any law requiring the collection;
- The main consequences (if any) if the information is not provided;
- How the individual may access and seek correction of information;
- How to make a complaint about a breach of the APPs and how the organization will deal with such complaint;
- Whether the information will be disclosed to an overseas recipient.

A company who is provided information from a third-party is obligated to provide the above information.

Sensitive information is not permitted to be collected by the company, unless:

- The individual has consented and the information is reasonably necessary for one or more of the entity's functions or activities;
- Collection is required or authorized by law;
- A permitted situation or health situation exists;

A company must, on request of an individual, give that individual access to the personal information that is held about the individual unless particular circumstances apply which allows the company to limit the extent to which access is given; including, emergency, business imperatives, law enforcement, and other public interests.

Transfer of Personal Information

Absent a limited exemption, personal information may only be disclosed to an organization outside of Australia where the entity has taken reasonable steps to ensure that the overseas recipient does not breach the APPs. However, the disclosing company will remain liable for an acts or omissions by the third-party.

Security of Personal Information

An organization must have appropriate security measures in place to protect personal information from misuse, loss, unauthorized access, modification or disclosure. The Privacy Commissioner issued guidance on establishing appropriate security measures.

An organization must also take reasonable steps to destroy or permanently de-identify personal information that is no longer needed.

Breach Notification

As of February 22, 2018, a company must notify the Office of the Australian Information Commissioner ("OAIC") and affected individuals of an "eligible data breach." An eligible data breach occurs when the following conditions are satisfied in relation to personal information:

- Both of the following are satisfied:
 - There is unauthorized access to, or unauthorized disclosure of, the information; and
 - A reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to which the information relates; or
- The information is lost in circumstances where:
 - Unauthorized access to, or unauthorized disclosure of, the information is likely to occur; and

- Assuming that unauthorized access or unauthorized disclosure were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to which the information relates.

A company must conduct, within **30 day**, an assessment if the company suspects (on reasonable grounds) that an eligible breach has occurred.

Notification is not required where law enforcement related activities are being carried out or where there is a written declaration by the Privacy Commission.

Enforcement

The Privacy Commissioner is tasked with enforcement. The Commissioner may issue a fine of up to A\$360,000 for an individual and A1.8 million for corporations.

VI. Austria

See GDPR discussion.

VII. Bahrain

Personal Data Protection, Law No. 30 (Official Gazette, July 2018)

On July 19, 2018, King Hamad bin Isa Al Khalifa ratified and issued Laws 30/2018, which will come into effect on August 1, 2019 (the Law on the Protection of Personal Data “LPPD”). Much of the LPPD will be explained when the regulations come into effect.

Application

The LPPD applies to:

- Every individual residing normally in Bahrain or having a workplace in Bahrain, and every legal person (corporate) having a place of business in the Kingdom of Bahrain; and
- Every individual not residing normally in Bahrain or having a workplace in Bahrain, and every legal person (corporate) not having a place of business in Bahrain, where such persons are processing data using means available in Bahrain.
 - According to the LPPD, a corporation is required to appoint an authorized representative in Bahrain, and notify the Data Protection Authority of such appointment.

Data Protection Officer

The LPPD contemplates a role of “Data Protection Supervisor” intended to act as an independent and impartial intermediary between the company and the Authority. This role will be expounded in the LPPD’s regulations.

Security Considerations

A company is required to apply technical and organization measures capable of protecting personal data against unintentional or unauthorized destruction, accidental loss, unauthorized alteration, disclosure or access, or any other form of processing.

The measures adopted need to be appropriate, bearing in mind the nature of the data in question and the risks associated with processing it. The company is required to maintain documentation that reflects the technical and organizational measures adopted, and must be available for viewing by parties concerned, as well as the Authority, any data processors, and the data controller itself.

The security considerations will be further expounded in the LPPD's regulations.

Breach Notification

No specific obligation in the LPPD. This may be expounded in the LPPD's regulations.

Enforcement

The LPPD imposes criminal penalties for violations. Penalties generally comprise up to one year in prison and/or a fine of between BHD1,000 and BHD20,000. The following are examples of activities that attract criminal penalties under the LPPD.

VIII. Belarus

Law on Information, Law No. 455 Z (2008)

Law on Population Register, Law No. 418 Z (2008)

The main legal acts regulating personal data protection in Belarus are the Law on Information ("IPL") and the Law on Population Register ("PRL"). In 2017, a new law on Personal Data was introduced and approved, and a draft is expected to be submitted to the parliament by April 2019. Belarus is not subject to the GDPR.

Personal Information

Personal information consists of name, surname, birth date, citizenship, and address details. There currently is no concept of sensitive personal information.

Data Protection Officer

A company shall establish special departments or select employees who are responsible for information protection.

Collection and Processing of Personal Information

A company collecting and processing personal information may only do so as follows:

- Must have written consent of the individual to whom the information belongs;
- Must be carried out in information systems equipped with information protection systems using technical or cryptographic means of protection;
- To be carried out having implemented certain legal, organizational, and technical measures for personal information protection.

Transfer of Personal Information

Transfer of personal information shall be carried out with written consent of the individual to whom the personal information belongs.

Security of Personal Information

A company using personal information shall carry out in accordance with Belarus law appropriate legal, organizational, technical measures of information in order to protect personal information.

Breach Notification

No breach notification provisions.

Enforcement

No present liability for the breach of the regulation on personal information protection. However, a fine may imposed, 20 basic units for individuals and up to 200 basic units for a company, for applying information protection systems and/or using technical and cryptographic means of protection that are not certified in accordance with Belarus law.

IX. Belgium

See GDPR discussion.

X. Bermuda

Personal Information Protection Act of 2016

The Personal Information Protection Act of 2016 “applies to every organization⁹³ that uses⁹⁴ personal information in Bermuda where that personal information is used wholly or partly by automated means and to the use other than by automated means of personal information which

⁹³ “Organization” means any individual, entity or public authority that uses personal information. PIPA, Part 1, Citation 2.

⁹⁴ “Use” or “using”, in relation to personal information, means carrying out any operation on personal information, including collecting, obtaining, recording, holding, storing, organizing, adapting, altering, retrieving, transferring, consulting, disclosing, disseminating or otherwise making available, combining, blocking, erasing or destroying it. PIPA, Part 1, Citation 2.

form, or are intended to form, part of a structured filing system.” Personal Information Protection Act (“PIPA”), Part 1, Citation 4.

Personal Information

“Personal information” means any information about an identified or identifiable individual. PIPA, Part 1, Citation 2.

Use of Personal Information

Under the PIPA, an organization may use an individual’s personal information if:

Consent: an organization must be able to reasonably demonstrate that the individual has knowingly consented;

Reasonableness: except in relation to sensitive personal information, a reasonable person giving due weight to the sensitivity of the personal information would consider—

- that the individual would not reasonably be expected to request that the use of his personal information should not begin or cease; and
- that the use does not prejudice the rights of the individual;

Contractual Necessity: it is necessary for the:

- for the performance of a contract to which the individual is a party; or
- for the taking of steps at the request of the individual with a view to entering into a contract;

Legal Requirement: the use of the personal information is pursuant to a provision of law that authorizes or requires such use;

Public Availability: the personal information is publicly available information and will be used for a purpose that is consistent with the purpose of its public availability;

Emergency: the use of the personal information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public;

Public Interest: the use of the personal information is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the organization or in a third party to whom the personal information is disclosed; or

Employment: the use of the personal information is necessary in the context of an individual’s present, past or potential employment relationship with the organization.

PIPA, Part 2, Citation 6. However, in order to comply with the PIPA, an organization must implement additional policies and practices regarding the protection of personal information, as well as make several operational changes.

Obligations on an Organization

The PIPA requires every organization to:

Suitable Measures and Policies: An organization must adopt suitable measures and policies to give effect to its obligations and to the rights of individuals set out in the PIPA, PIPA Part 2, Citation 5(1);

- The suitable measures and policies shall “take into account the nature, scope, context and purpose of the use of personal information and the risk to individuals by the use of the personal information,” PIPA, Part 2, Citation 5(2).

Privacy Officer: An organization must designate a representative (“privacy officer”) to ensure compliance with PIPA and for communicating with the Commissioner, PIPA, Part 2, Citation 5(4).

Third Parties: Where an organization engaged (by contract or otherwise) the services of a third party in connection with the use of personal information, the organization remains responsible for compliance with the PIPA at all times, PIPA, Part 2, Citation 5(3).

Fairness: The PIPA requires an organization to use personal information in a “lawful and fair” manner. PIPA, Part 2, Citation 8.

Proportionality: An organization shall “ensure that personal information is adequate, relevant and not excessive in relation to the purpose for which it is used,” PIPA, Part 2, Citation 11.

Privacy Notices: An organization using an individual’s personal information “shall provide the individuals with a clear and easily accessible statement about its practices and policies with respect to personal information.” PIPA, Part 2, Citation 9(1). This includes:

- the fact that personal information is being used;
- the purposes for which personal information is or might be used;
- the identity and types of individuals or organizations to whom personal information might be disclosed;
- the identity and location of the organization, including information on how to contact it about its handling of personal information;
- the name of the privacy officer;
- the choices and means the organization provides to an individual for limiting the use of, and for accessing, rectifying, blocking, erasing and destroying, his personal information.

PIPA, Part 2, Citation 9(1)(a)–(f). However, the privacy notice is **not** required if:

- the personal information is publicly available information; or
- the organization can “reasonably determine that all uses made, or to be made, of the personal information are within the reasonable expectations of the individual to whom the personal information relates.”

PIPA, Part 2, Citation 9(3)(a)–(b).

Integrity of Personal Information: An organization “shall ensure that any personal information used is accurate and kept up to date” for its intended purpose. PIPA, Part 2, Citation 12(1). Additionally, the personal information shall not be “kept for longer than is necessary” for the purpose of use. PIPA, Part 2, Citation 12(2).

Security Safeguards: The PIPA requires an organization to protect personal information with appropriate safeguards against risk, including:

- loss;
- unauthorized access, destruction, use, modification or disclosure; and
- any other misuse.

PIPA, Part 2, Citation 13(1)(a)–(c). These safeguards are subject to periodic review and shall be proportional to risk of loss, access, or misuse of the personal information, the sensitivity of the information, and the context in which it is held. PIPA, Part 2, Citation 13(2)(a)–(c).

Categories of Information

Sensitive Information: Sensitive information⁹⁵ is held to a higher account and cannot be used to discriminate against any person contrary to the provisions of Part II of the Human Rights Act of 1981 without lawful authority. PIPA, Part 2, Citation 7. Sensitive information is used with lawful authority if an only to the extent that it is used –

- with the consent of any individual to whom the information relates;
- in accordance with an order made by either the court or the Commissioner;
- for the purpose of any criminal or civil proceedings; or

⁹⁵ “Sensitive personal information” means any personal information relating to an individual’s place of origin, race, color, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information.

- in the context of recruitment or employment where the nature of the role justifies such use.

PIPA, Part 2, Citation 7.

Personal Information – Children: Verifiable consent must be obtained from the parent/guardian before the personal information of a child (defined as under 14 years) is collected or otherwise used and privacy notices must be age appropriate. PIPA, Part 2, Citation 16.

Access

At the request of an individual for access to his personal information, an organization shall provide the individual with access to:

- personal information about the individual in the custody or control of the organization;
- the purpose for which the information has been and is being used; and
- the names of the persons or types of person to whom and circumstances in which the personal information has been and is being disclosed.

PIPA, Part 3, Citation 17(1). An organization may refuse to provide access to the personal information if:

Legal Privilege: the information is protected by any legal privilege;

Confidential Information: the information would reveal confidential information of the organization or of a third party that is of a commercial nature and it is not unreasonable to withhold that information;

Disciplinary/Criminal Investigation/Legal Proceedings: the personal information is being used for a current disciplinary or criminal investigation or legal proceedings, and refusal does not prejudice the right of the individual to receive a fair hearing;

Mediation/Arbitration: the personal information was used by a mediator or arbitrator, or was created in the conduct of a mediation or arbitration for which the mediator or arbitrator was appointed to act under an agreement or by a court;

Business Negotiations: the disclosure of the personal information would reveal the intentions of the organization in relation to any negotiations with the individual to the extent that the provision of access would be likely to prejudice those negotiations.

PIPA, Part 3, Citation 17(2). An organization shall not provide access to personal information if:

- the disclosure of the personal information could reasonably be expected to threaten the life or security of an individual;
- the personal information would reveal personal information about another individual; or

- the personal information would reveal the identity of an individual who has in confidence provided an opinion about another individual and the individual providing the opinion does not consent to disclosure of his identity.

PIPA, Part 3, Citation 17(3).

Transfer of Personal Information Out of the Jurisdiction

If an organization transfers personal information for use by an overseas third party, the organization remains responsible for compliance with the PIPA. PIPA, Part 2, Citation 15(1). Prior to transferring the personal information, the organization shall assess the level of protection by the overseas third party. PIPA, Part 2, Citation 15(2)–(5).

Disclosure for Purpose of Business Transaction

Organizations that are parties to a business transaction may use personal information about a person without the consent of the person if:

- the parties have entered into an agreement under which the use of the personal information is restricted to those purposes that relate to the business transaction; **and**
- the personal information is necessary
 - For the parties to determine whether to proceed with the business transaction; and
 - If the determination is to proceed with the business transaction, for the parties to carry out and complete the business transaction.

PIPA, Part 6, Citation 46 (3)(a). Where the business transaction is completed, the organizations may use personal information about a person without the consent of the person if:

- the parties have entered into an agreement under which the parties undertake to use and disclose information only for those purposes for which the personal information as initially collected from or in respect of those persons; and
- the information relates solely to the carrying on of the business or activity or the carrying out of the objects for which the business transaction took place.

PIPA, Part 6, Citation 46 (3)(b). If a business transaction does not proceed or is not completed, the party to whom the personal information was disclosed shall either destroy the personal information or turn it over to the party which disclosed the personal information. PIPA, Part 6, Citation 46 (3)(b).

Breach of Security

If a breach of security is likely to adversely affect an individual, the organization must notify the Privacy Commissioner and any individual affected by the breach. PIPA, Part 2, Citation 13(1)(a)–

(b). The notification shall include: (1) the nature of the breach, (2) its likely consequences for that individual, and the measures being taken to address the breach. PIPA, Part 2, Citation (2)(a)–(c).

Enforcement

The Privacy Commission is responsible for monitoring how the PIPA is administered and to ensure that its purposes are achieved. A person commits an offense under the PIPA if:

- willfully or negligently uses or authorize the use of personal information in a manner that is inconsistent with Part 2 and is likely to cause harm to an individual or individuals;
- willfully attempts to gain or gains access to personal information in a manner that is inconsistent with this Act and is likely to cause harm to an individual or individuals;
- disposes of or alters, falsifies, conceals or destroys personal information;
- obstructs the Commission or an authorized delegate of the Commission in the performance of the Commissioner’s duties, powers or functions under the PIPA;
- knowingly makes a false statement to the Commissioner or knowingly misleads or attempts to mislead the Commissioner in the course of the Commissioner’s performance of the Commissioner’s duties, powers or functions under the PIPA;
- knowingly or recklessly fails to comply with restrictions on disclosure of information by the Commissioner;
- fails to comply with an order made by the Commissioner;
- fails to comply with a notice served by the Commissioner;
- contravenes the sensitive personal information section;
- disposes of, alters, falsifies, conceals or destroys evidence during an investigation or inquiry by the Commissioner; or
- fails to notify a breach of security to the Commissioner.

PIPA, Part 6, Citation 47(1). A person committing an offense may be liable:

- on summary conviction, in the case of an individual, to a fine of up to \$25,000 and/or to two years imprisonment; and
- on conviction on indictment, in the case of a person other than an individual, to a fine not exceeding \$250,000.00.

PIPA, Part 6, Citation 47.

XI. Bosnia and Herzegovina

Law on the Protection of Personal Data (“Official Gazette of BiH; No.: 49/06)

The Law on Protection of Personal Data (“PD Law”) is the governing law regulating data protection issues in Bosnia and Herzegovina.

Personal Information

The PD Law defines personal information as any information relating to an identified or identifiable natural person. Sensitive Personal data is defined as relating to:

- Racial, national or ethnic origin;
- Political opinion, party affiliation, or trade union affiliation;
- Religious, philosophical or other belief;
- Health;
- Genetic code;
- Sexual life;
- Criminal convictions; and
- Biometric data.

Registration

A company must provide the Personal Data Protection Agency (“PDPA”) with specific information on the database containing personal information. The forms can be located on the PDPA website.

Data Protection Officer

Not required by the PD Law.

Collection & Processing of Personal Information

Collection and processing of personal information is permissible with the individual’s consent and if obtained in compliance with the basic principles of data protection.

The consent for the collection and processing of personal information falling within the general personal category of personal information does not have to be in writing. However, the collection of sensitive personal information requires explicit written consent from the individual.

A company is also required to adhere to principles of personal data processing, which are:

- Process personal data fairly and lawfully;
- Process personal data collected for special, explicit and lawful purposes in no manner contrary to the specified purpose;
- Process personal data only to the extent and scope necessary for the fulfilment of the specified purpose;
- Process only authentic and accurate personal data, and update such data when necessary;
- Erase or correct personal data which are incorrect and incomplete, given the purpose for which the data are collected or further processed;
- Process personal data only within the period of time necessary for the fulfilment of the purpose of their processing;
- Keep personal data in the format that allows identification of the data subject for not longer than required for the purpose for which the data are collected or further processed;
- Ensure that personal data that were obtained for various purposes are not combined or merged.

Consent is **not required** if the processing is necessary for the fulfilment of a company's statutory obligation or for preparation or realization of an agreement concluded between a company and an individual.

Transfer of Personal Information

Processed personal information may be transferred to countries where an adequate level of person protection is ensured. Certain exceptions apply as stipulated by the DP Law.

Security of Personal Information

The DP Law prescribes that both a company and, within the scope of their competencies, the processors are required:

- To take care of data security and to undertake all technical and organizational measures;
- To undertake measures against unauthorized or accidental access to personal data, their alteration, , destruction or loss, unauthorized transfer, other forms of illegal data processing, as well as measures against misuse of personal information; and
- To adopt a personal data security plan, which must include the categories of processed data and the list of instruments for protection to ensure confidentiality, integrity, availability, authenticity, possibility of revision, and transparency of the personal information.

A company is required to undertake more stringent technical and organizational measures when processing sensitive personal information.

Breach Notification

The DP Law does not impose a duty to notify in the case of a breach.

Enforcement

The PDPA may initiate a misdemeanor proceeding against a company, depending on the gravity of the offense. The offences and sanctions include monetary fines in the amount between EUR 2,550 and EUR 51,100, as well as for the company's authorized representative in the amount between EUR 100 and EUR 7,700.

Breach of personal information protection regulations also represents a criminal offense of unauthorized collection of personal information. Prescribed sanctions are monetary fines in amount to be determined by the court or imprisonment of up to six (6) months.

XII. Brazil

Lei Geral de Protecao de Dados, Law 13,709 (2018)

In August 2018, Brazil enacted Lei Geral de Protecao de Dados (Law 13,709/2018) ("LGPD"). The LGPD is expected to come into force in February 2020. Similarly to the GDPR, the LGPD is applicable to companies "irrespective of . . . the county in which [an entity's] headquarters is located or the country where the data are located," if the data processing happens in Brazil, if the purpose of the processing is to offer or provide goods or services in Brazil, or if the data being processed is collected in Brazil.

Personal Information

Personal information is defined as "information related to an identified or identifiable individual." Like the GDPR and the new California Consumer Privacy Act, the LGPD aims to reach information that could be used to identify a person even if the information on its face does not do so.

Sensitive data is "personal data related to one's racial or ethnic origin, religious, philosophical or political affiliations, health, and sexual, biometric or genetic data."

Data Protection Officer

A company shall appoint a data protection officer responsible for receiving complaints and communications, and for providing orientation within the company on best practices.

Collection & Processing of Personal Information

A company shall observe the good faith and the following principles:

- Purpose: processing for legitimate, specific and explicit purposes informed to the data subject, without any possibility of subsequent processing inconsistent with these purposes;
- Adequacy: Compatibility of the processing with the purposes informed to the data subject;
- Need: limitation of the processing to the minimum processing required for achievement of its purposes, encompassing pertinent, proportional and non-excessive data in relation to the purposes of the data processing;

- Free access: guarantee, to the data subjects, of facilitated and free consultation on the form and duration of the processing, as well as all their personal data;
- Quality of data: guarantee, to the data subjects, of accuracy, clarity, relevance and update of the data, according to the need and for compliance with the purpose of the processing;
- Transparency: guarantee, to the data subjects, of clear, accurate and easily accessible information on the processing and the respective processing agents, subject to business and industrial secrets;
- Security: use of technical and administrative measures able to protect the personal data from unauthorized access and from accidental and unlawful situations of destructions, loss, alteration, communication or diffusion;
- Prevention: adoption of measures to prevent the occurrence of damage in view of the processing of personal data;
- Non-discrimination: impossibility of processing data for discriminatory, unlawful or abusive purposes;
- Liability and accounting: proof, by the agent, of adoption of effective measures able to prove observance of and compliance with the personal data protection rules, and also with the effectiveness of these measures.

A company may only process personal information if one of the following events:

- Consent;
 - Must be provided in writing or by other means that proves the manifestation of will of the data subject;
 - If in writing, must be in a clause separated from the other contractual clauses.
- Fulfillment of legal, regulatory or contractual obligations;
- For the conduction of studies by research bodies, guaranteed, whenever possible, the anonymization of personal data;
- For the protection of the life or of the physical safety of the data subject;
- For the protection of the health, in a procedure carried out by health professionals;
- Whenever necessary to serve the legitimate interests of the controller or of third parties.

Sensitive personal information may only be processed with consent or in any of the following (relevant) situations:

- Compliance with statute;

- The conduction of studies by a research body, guaranteeing, whenever possible, anonymization of the data;
- Protection of the life or of the physical safety of the data subjects or of third parties;
- Protection of health, in a procedure carried out by health professionals.

A company must inform, correct, anonymize, delete or provide a copy of the data if requested by the data subject. Additionally, a company must delete data after the relevant relationship terminates, unless expressly permitted to retain the data.

Transfer of Personal Information

The general rule under the LDGP is that transfer of personal information is prohibited, absent certain enumerated exceptions. The relevant exceptions are as follows:

- If the receiving country or organization provides a level of data protection comparable to the LGPD's;
- The parties are bound by contract or by global corporate policy to provide and demonstrate a level of data protection comparable to the LGPD's;
- For international legal cooperation between government agencies; and
- Where the data subject has given specific consent to the transfer, "distinct from other purposes."

Security of Personal Information

A company shall adopt security, technical and administrative measures that are capable of protecting the personal data from unauthorized access and accidental or unlawful situations of destruction, loss, modification, communication or any form of inappropriate or unlawful processing.

Breach Notification

A company shall notify the supervisory authority and the data subject of the occurrence of any security incident that may result in any relevant risk or damage to the data subjects.

Enforcement

Under the LGPD, violations are subject to penalties ranging from warnings to fines up to 2 percent of the company's gross revenue in Brazil in the previous year, limited to 50 million reais per violation.

XIII. Bulgaria

See GDPR discussion.

XIV. Canada

There are four private sector privacy statutes that govern the collection, use, disclosure, and management of personal information in Canada: (1) the Federal Personal Information Protection and Electronic Documents Act; (2) Alberta's Personal Information Protection Act; (3) British Columbia's Personal Information Protection Act; and (4) Quebec's An Act Respecting the Protection of Personal Information in the Private Sector.

A. The Federal Personal Information Protection and Electronic Documents Act

Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.)

Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA") is the federal privacy law for private-sector organizations. It sets out the ground rules for how business must handle personal information in the course of commercial activity.

The federal government may exempt from PIPEDA organizations and/or activities in provinces that have adopted substantially similar privacy legislation. To date, Quebec, British Columbia and Alberta have adopted private sector legislation deemed substantially similar to the PIPEDA. Further, Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia have adopted substantially similar legislation with respect to personal health information.

Even in those provinces that have adopted legislation that is substantially similar to the federal privacy legislation, PIPEDA continues to apply to (i) all interprovincial and international transactions by all organizations subject to the Act, and (ii) to federally regulated organizations — "federal works, undertakings or businesses" — such as banks, and telecommunications and transportation companies, in the course of their commercial activities.

General

What is a Commercial Activity?

Commercial activity means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists. PIPEDA 2(1).

What is Personal Information?

Personal information means information about an identifiable individual. PIPEDA 2(1) This includes information in any form, such as:

- Age, name, ID numbers, income, ethnic origin, or blood type;
- Opinions, evaluations, comments, social status, or disciplinary actions; and

- Employee files, credit reports, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions.

Application

The PIPEDA applies to every organization in respect of personal information that:

- the organization collects, uses or discloses in the course of commercial activities; or
- is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

Principles

The PIPEDA establishes ten principles which have to be embodied in every organization's privacy regime in order for the organization to be in compliance. The ten principles are:

- Accountability;
- Identify Purpose;
- Consent;
- Limiting Collection;
- Limiting Use, Retention, and Disclosure;
- Accuracy;
- Safeguards;
- Openness;
- Individual Access;
- Ability to Challenge Compliance.

In addition to the ten principles, the PIPEDA contains an overriding obligation that any collection, use or disclosure of personal information must only be for purposes that a **reasonable person would consider appropriate under the circumstances**.

Accountability (1)

Privacy Officer

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organizations compliance with all principles. The individual(s) shall be made known upon request.

Third Parties

The organization is responsible for the personal information in its possession or custody, including information that has been transferred to third party for processing. The organization shall use contractual or other means to provide a comparable level of protection.

Policies and Practices

The organization shall implement policies and practices to give effect to the principles, including

- Implementing procedures to protect personal information;
- Establishing procedures to receive and respond to complaints and inquiries;
- Training staff and communicating to staff information about the organization's policies and practices; and
- Developing information to explain the organization's policies and procedures.

Identifying Purposes (2)

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Disclosure

The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done **orally or in writing**.

New Purpose

Any new purposes shall be identified prior to use.

Consent (3)

Consent is considered valid only if it is reasonable to expect that individuals to whom an organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure, to which they are consenting.

Responsibilities:

- Specify what personal information you are collecting and why in a way that your customers and clients can clearly understand.
- Inform the individual in a meaningful way of the purposes for the collection, use or disclosure of personal data.
- Obtain the individual's consent before or at the time of collection, as well as when a new use of their personal information is identified.

How to fulfill these responsibilities:

- Obtain informed consent from the individual whose personal information is collected, used or disclosed.

- Explain how the information will be used and with whom it will be shared. This explanation should be clear, comprehensive, and easy to find. Retain proof that consent has been obtained.
- Never obtain consent by deceptive means.
- Do not deny a product or service to an individual who fails to consent to the collection, use or disclosure of information *beyond* that required to fulfill an explicitly specified and legitimate purpose.
- Explain to individuals the implications of withdrawing their consent.
- Ensure that employees collecting personal information are able to answer individuals' questions about why they are being asked for this information.

EXCEPTIONS TO THE CONSENT PRINCIPLES

Collection of personal information without knowledge or consent:

An organization may collect personal information **without** the knowledge or consent of the individual only if:

- the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;
- it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;
- it is contained in a witness statement and the collection is necessary to assess, process or settle an insurance claim;
- it was produced by the individual in the course of their employment, business or profession and the collection is consistent with the purposes for which the information was produced;
- the collection is solely for journalistic, artistic or literary purposes;
- the information is publicly available and is specified by the regulations; or
- the collection is made for the purpose of making a disclosure
 - under subparagraph (3)(c.1)(i) or (d)(ii), or
 - that is required by law.

Use personal information without knowledge or consent:

An organization may, **without** the knowledge or consent of the individual, use personal information only if:

- in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of

the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention;

- it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual;
- the information is contained in a witness statement and the use is necessary to assess, process or settle an insurance claim;
- the information was produced by the individual in the course of their employment, business or profession and the use is consistent with the purposes for which the information was produced;
- it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used;
- it is publicly available and is specified by the regulations; or
- it was collected under paragraph (1)(a), (b) or (e).

Disclosure of personal information without knowledge or consent:

An organization may disclose personal information **without** the knowledge of consent of the individual only if the disclosure is:

- made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization;
- for the purpose of collecting a debt owed by the individual to the organization;
- required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;
- made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that
 - it suspects that the information relates to national security, the defense of Canada or the conduct of international affairs,
 - the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law,
 - the disclosure is requested for the purpose of administering any law of Canada or a province, or

- the disclosure is requested for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual;
- made to the government institution mentioned in section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* as required by that section;
- made on the initiative of the organization to a government institution or a part of a government institution and the organization
 - has reasonable grounds to believe that the information relates to a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or
 - suspects that the information relates to national security, the defense of Canada or the conduct of international affairs;
- made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation;
- made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud;
- made on the initiative of the organization to a government institution, a part of a government institution or the individual's next of kin or authorized representative and
 - the organization has reasonable grounds to believe that the individual has been, is or may be the victim of financial abuse,
 - the disclosure is made solely for purposes related to preventing or investigating the abuse, and
 - (it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the ability to prevent or investigate the abuse;
- necessary to identify the individual who is injured, ill or deceased, made to a government institution, a part of a government institution or the individual's next of kin or authorized representative and, if the individual is alive, the organization informs that individual in writing without delay of the disclosure;
- made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure;
- of information that is contained in a witness statement and the disclosure is necessary to assess, process or settle an insurance claim;

- of information that was produced by the individual in the course of their employment, business or profession and the disclosure is consistent with the purposes for which the information was produced;
- for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the Commissioner of the disclosure before the information is disclosed;
- made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation;
- made after the earlier of
 - one hundred years after the record containing the information was created; and
 - twenty years after the death of the individual whom the information is about;
- of information that is publicly available and is specified by the regulations; or
- as required by law.

Use and disclosure of personal information without knowledge or consent in a prospective business transaction:

Organizations that are parties to a prospective business transaction may use and disclose personal information **without** the knowledge or consent of the individual if:

- the organizations have entered into an agreement that requires the organization that receives the personal information
 - to use and disclose that information solely for purposes related to the transaction;
 - to protect that information by security safeguards appropriate to the sensitivity of the information; and
 - if the transaction does not proceed, to return that information to the organization that disclosed it, or destroy it, within a reasonable time; and
- the personal information is necessary
 - to determine whether to proceed with the transaction; and
 - if the determination is made to proceed with the transaction, to complete it.

Use and disclosure of personal information without knowledge or consent in a prospective business transaction:

Organizations that are parties to the transaction may use and disclose personal information, which was while a prospective business transaction, **without** the knowledge or consent of the individual if:

- the organizations have entered into an agreement that requires each of them

- to use and disclose the personal information under its control solely for the purposes for which the personal information was collected, permitted to be used or disclosed before the transaction was completed;
- to protect that information by security safeguards appropriate to the sensitivity of the information; and
- to give effect to any withdrawal of consent made under clause 4.3.8 of Schedule 1;
- the personal information is necessary for carrying on the business or activity that was the object of the transaction; and
- one of the parties notifies the individual, within a reasonable time after the transaction is completed, that the transaction has been completed and that their personal information has been disclosed under subsection (1).

Limiting Collection (4)

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by **fair and lawful** means.

Responsibilities:

Organizations should not collect personal information discriminately. Do not deceive or mislead individuals about the reasons for collecting personal information.

Limiting Use, Disclosure and Retention (5)

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Responsibilities:

- Organizations using personal information for a new purpose shall document this purpose.
- Organizations should develop guidelines and implement procedures with respect to the retention of personal information.
 - These should include minimum and maximum retention periods.
- Personal information that is no longer required to fulfill the identified purpose should be destroyed, erased, or made anonymous. Organizations should develop guidelines and implement procedures for the destruction of personal information.

Accuracy (6)

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Responsibilities:

- The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual.
- An organization shall not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected.
- Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

Safeguards (7)

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Responsibilities:

- The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.
- The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection.
- Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

NOTE: The PIPEDA does not provide specific guidelines for the safeguarding of personal information.

Openness (8)

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Responsibilities:

- Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.
- The information made available shall include
 - the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
 - the means of gaining access to personal information held by the organization;
 - a description of the type of personal information held by the organization, including a general account of its use;

- a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
 - what personal information is made available to related organizations (e.g., subsidiaries).
- An organization may make information on its policies and practices available in a variety of ways.

Individual Access (9)

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Responsibilities:

- Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information.
- An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
 - When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.
- The organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.
- An organization shall respond to an individual's request within **thirty days** after receipt of the request and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable.
 - An organization may extend the time limit for a maximum of thirty days if:
 - Meeting the time limit would unreasonably interfere with the activities of the organization, or
 - The time required to undertake any consultations necessary to respond to the request would make the time limit impracticable to meet; or
 - For the period that is necessary in order to be able to convert the personal information into an alternative format.
 - An organization may respond to an individual's request at a cost to the individual only if
 - The organization has informed the individual of the approximate cost; and
 - The individual has advised the organization that the request is not being withdrawn.

Challenging Compliance (10)

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Responsibilities:

- Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information.
 - The complaint procedures should be easily accessible and simple to use.
- Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures.
- An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

Remedies

The PIPEDA does not create an automatic right to sue for violations of the law's obligations. Instead, the PIPEDA allows for complaints to be taken to the Office of the Privacy Commissioner of Canada. The Commissioner is then required to investigate the complaint and produce a report at its conclusion. The Commissioner does not have any powers to order compliance, award damages or levy penalties.

A complainant may, after receiving the Commissioner's investigation report, apply to the Federal Court of Canada for a hearing with respect to the subject matter of the complaint. The Court may, in addition to any other remedies it may give,

- Order an organization to correct its practices;
- Order an organization to publish a notice of any action taken or proposed to be taken to correct its practices; and
- Award damages to the complainant, including damages for any humiliation that the complainant has suffered.

Breach Notifications

The Canadian government published the final regulations relating to the mandatory reporting of privacy breaches under the PIPEDA. In June 2015, Canada passed Bill S-4 – The Digital Privacy Act— into law, and the provisions will take force on November 1, 2018.

Breaches of Security Safeguards

An organization shall report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the

breach creates a real risk of significant harm to an individual. An organization shall **also** notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

- "Breach of security safeguards" means the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards or from a failure to establish those safeguards.
- "Significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

Relevant factors to consider when determining whether a breach of security safeguards creates a real risk of significant harm include:

- The sensitivity of the personal information involved in the breach;
- The probability that the personal information has been, is being or will be misused; and
- Any other prescribed factor.

Report to Commissioner

A report of a breach of security safeguards must be in writing, sent by a secure means of communications, and must contain:

- a description of the circumstances of the breach and, if known, the cause;
- the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period;
- a description of the personal information that is the subject of the breach to the extent that the information is known;
- the number of individuals affected by the breach or, if unknown, the approximate number;
- a description of the steps that the organization has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm;
- a description of the steps that the organization has taken or intends to take to notify affected individuals of the breach in accordance with subsection 10.1(3) of the Act; and
- the name and contact information of a person who can answer, on behalf of the organization, the Commissioner's questions about the breach.

An organization may submit to the Commissioner any new information that the organization becomes aware of after having made the report.

Notification to Affected Individual

A notification provided by an organization to an affected individual with respect to a breach of security safeguards must contain:

- a description of the circumstances of the breach;
- the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;
- a description of the personal information that is the subject of the breach to the extent that the information is known;
- a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach;
- a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and
- contact information that the affected individual can use to obtain further information about the breach.

Direct notification must be given to the affected individual in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstance. **Indirect notification** must be given in any of the following circumstances:

- direct notification would be likely to cause further harm to the affected individual;
- direct notification would be likely to cause undue hardship for the organization; or
- the organization does not have contact information for the affected individual.

Indirect notification must be given by public communication or similar measure that could reasonably be expected to reach the affected individuals.

Notification to Other Organizations:

An organization that notifies an individual of a breach of security safeguards shall notify any other organization, a government institution or a part of a government institution of the breach if the notifying organization believes that the other organization or the government institution or part concerned may be able to reduce the risk of harm that could result from it or mitigate that harm, or if any of the prescribed conditions are satisfied.

Record Keeping

An organization shall keep and maintain a record of every breach of security safeguards involving personal information under its control for twenty-four months after the day on which the organization determines that the breach occurred. This means that regardless of whether the breach notification threshold is triggered, an organization must maintain a record of every such breach for a period of 24 months from the day that the organization determines that a breach occurred. These records must be provided to the Commissioner upon request and they must contain sufficient information to allow the Commissioner to verify compliance with PIPEDA's breach reporting provisions.

Penalties

In order to enforce these new breach reporting and record-keeping requirements, PIPEDA now includes financial penalties. Specifically, if an organization knowingly violates either of these requirements, it will face fines of up to \$100,000. While these financial penalties in

no way come close to the prospective penalties under the GDPR, they clearly ‘add teeth’ to the above-noted requirements.

B. Alberta’s Personal Information Protection Act

Alberta’s Personal Information Protection Act, SA 2003, c P-6.5 (Can.)

The purpose of Alberta’s Personal Information Protection Act (“APIPA”) is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of the individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable.

Application

The APIPA applies to every organization and in respect of all personal information.

What is personal information?

Personal information means information about an identifiable individual.

Standard to be applied -- reasonableness?

The standard to be applied under this Act is what a **reasonable** person would consider appropriate in the circumstances.

Compliance

Under the APIPA, an organization:

- Is responsible for personal information that is in its **custody or under its control**;
- Responsible for the **third-party** compliance with the APIPA;
- Must **designate** one or more individuals to ensure compliance with the APIPA; and
- Must act in a **reasonable** manner.

Policies and Practices

An organization must **develop and follow** policies and practices that are reasonable for the organization to meet. This information must be available on request.

Consent

An organization **shall not**, with respect to personal information and without the **consent**:

- Collect information;
- Collect information from another source;
- Use information; or
- Disclose information.

An organization **shall not** require an individual consent to the collection, use or disclosure of personal information **beyond what is necessary** to provide the product or service.

Form of Consent

Consent conforms to the APIPA in any of the following circumstances:

- An individual may give consent **in writing** or **orally** to the collection, use or disclosure of personal information.
- An individual is deemed to have consented if they **voluntarily** provide the information and it is **reasonable** to prove that information.
- An organization may also collect, use or disclosure personal information about an individual for a particular purpose if:
 - The organization provides the individual with (1) **notice** and (2) gives the individual a **reasonable opportunity** to decline or object;
 - The individual **does not** object or decline; and
 - It is reasonable to collect having regard to the level of **sensitivity** of the information.

Withdrawal or Variation of Consent

On giving reasonable notice to an organization, an individual may **at any time, withdraw or vary consent** to the collection, use or disclosure by the organization of personal information about the individual.

An organization then **must** inform the individual of the likely **consequences** to the individual of withdrawing or varying the consent, **unless** the consequences are reasonably obvious.

Upon receipt of the withdrawal or variation of consent, an organization must:

- Stop collecting, using or disclosing; and
- In the case of variation, abide by the variation.

Collection of Personal Information

Limitations

An organization may collect personal information only for purposes that are **reasonable**, and only to the extent that is **reasonable** for meeting the purposes.

Notification Required for Collection

Before or at the time of collecting personal information, an organization must notify that individual in writing or orally:

- The **purpose** for which the information is collected; and
- The **name/position name/ title of a person** able to answer on behalf of the organization questions about collection.

Third Party: **Before or at the time** personal information is collected from another organization without the consent of an individual, the organization collecting must provide the organization with sufficient information regarding the purpose for which the information is being collected.

Notification Respecting Service Provider Outside of Canada

An organization that uses a service provider outside of Canada to collect personal information with consent or an organization that, directly or indirectly, transfers to a service provider outside of Canada must notify the individual **before or at the time of collecting or transferring the information**, in writing or orally of:

- The way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside of Canada; and
- The **name/position name/ title of a person** able to answer on behalf of the organization questions about collection.

Collection Without Consent

An organization may collect personal information about an individual **without consent** but only if one or more of the following are applicable (irrelevant exceptions omitted):

- **Reasonable:** Collection is reasonable considering the individual's interest, time, and likelihood of withholding consent;
- **Authorization:** Authorized by statute, regulation, bylaw, or legislative instruction, or form pursuant to statute;
- **Legal Proceedings:** Reasonable for the purpose of an investigation or a legal proceeding;
- **Publicly Available Information:**

- **Emergency**: The use of the information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public.

Collection of Employee Information

An organization may collect personal employee information about an individual **without consent** if:

- The information is used solely for the purpose of:
 - Establishing, managing or terminating an employment or volunteer-work relationship, or
 - Managing a post-employment or post-volunteer-work relationship;

Between the organization and the individual;

- It is reasonable to use the information for the particular purpose for which it is being used; and
- In the case of a current employee, the organization has, before using the information, provided reasonable notification.

Use of Personal Information

Limitations

An organization may use personal information only for purposes that are **reasonable**, and only to the extent that is **reasonable** for meeting the purposes.

Use Without Consent

An organization may use personal information about an individual **without consent** but only if one or more of the following are applicable (irrelevant exceptions omitted):

- **Reasonable**: Collection is reasonable considering the individual's interest, time, and likelihood of withholding consent;
- **Authorization**: Authorized by statute, regulation, bylaw, or legislative instruction, or form pursuant to statute;
- **Legal Proceedings**: Reasonable for the purpose of an investigation or a legal proceeding;
- **Publicly Available Information**;
- **Emergency**: The use of the information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public.

Use of Employee Information

An organization may use personal employee information about an individual **without consent** if:

- The information is used solely for the purpose of:
 - Establishing, managing or terminating an employment or volunteer-work relationship; or
 - Managing a post-employment or post-volunteer-work relationship;

Between the organization and the individual;

- It is reasonable to use the information for the particular purpose for which it is being used; and
- In the case of a current employee, the organization has, before using the information, provided reasonable notification.

Disclosure of Personal Information

Limitations

An organization may disclose personal information only for purposes that are **reasonable**, and only to the extent that is **reasonable** for meeting the purposes.

Disclosure Without Consent

An organization may disclose personal information about an individual **without consent** but only if one or more of the following are applicable (irrelevant exceptions omitted):

- **Reasonable**: Collection is reasonable considering the individual's interest, time, and likelihood of withholding consent;
- **Authorization**: Authorized by statute, regulation, bylaw, or legislative instruction, or form pursuant to statute;
- **Legal Proceedings**: the disclosure of the information is for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction to compel the production;
- **Law Enforcement**: To assist in an investigation undertaken with a view to a law enforcement proceeding, or from which a law enforcement proceeding is likely to result;
- **Publicly Available Information**;

- **Emergency**: The use of the information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public.

Use of Employee Information

An organization may disclose personal employee information about an individual **without consent** if:

- The information is used solely for the purpose of:
 - Establishing, managing or terminating an employment or volunteer-work relationship; or
 - Managing a post-employment or post-volunteer-work relationship;

Between the organization and the individual;

- It is reasonable to use the information for the particular purpose for which it is being used; and
- In the case of a current employee, the organization has, before using the information, provided reasonable notification.

Business Transactions

An organization may, for purposes of the business transaction between itself and one or more other organizations, collect, use and disclose personal information in accordance with this section.

Organizations that are parties to a business transaction may,

- During the period leading up to and including the completion, if any, of any business transaction, collect, use and disclose personal information **without consent** if:
 - The parties have entered into an agreement under which the collection, use and disclosure of the information is restricted for purposes that relate to the business; and
 - The information is necessary
 - For the parties to determine whether to proceed with the business transaction; and
 - If the determination is to proceed with the business transaction, for the parties to carry out and complete it; and
 - Where the business transaction is completed, collect, use and disclose personal information about individual without the consent of the individuals if

- The parties have entered into an agreement under which the parties undertake to use and disclose the information only for those purposes for which the information was initially collected from or in respect of the individuals; and
- The information relates solely to the carrying on of the business or activity or the carrying out of the objects for which the business transaction took place.

If the business transaction does not proceed or is not completed, the party whom the information was disclosed, if in the custody or control, must either **destroy** or **turn it over** to the party that disclosed the information.

Access to and Correction and Care of Personal information

Access and Correction

Access

An individual may request an organization:

- Provide the individual with **access** to personal information about the individual; or
- To provide the individual with **information about the use or disclosure** of personal information.

On request for **access** to information, and taking into consideration what is **reasonable**, an organization must provide the applicant with access where the information is **contained in a record** that is in the **custody** or **control** of the organization.

On request for **information** about **use or disclosure**, and taking into consideration what is **reasonable**, an organization must, if in its custody or control, provide the applicant with:

- Information about the process for which the information has been and is being used; and
- The names of the persons to whom and circumstances in which the personal information has been and is being disclosed.

An organization **may refuse** to provide access to personal information if:

- The information is protected by any legal privilege;
- Disclosure would reveal confidential information that is of a commercial nature and it is not unreasonable to withhold;
- The information was collected for an investigation or legal proceeding;

- The disclosure may result in that type of information no longer being provided to the organization when it is reasonable that that type of information would be provided;
- The information was collected by a mediator;
- The information relates to or may be used in the exercise of prosecutorial discretion.

An organization **shall not** provide access if:

- Disclosure could reasonably be expected to threaten the life or security of another;
- Disclosure would reveal information about another;
- Disclosure would reveal the identity of an individual who in confidence provided an opinion about another individual, and does not consent to his/her disclosure.

Right to Request Correction

An individual **may** request an organization to correct an error or omission in the personal information about the individual that is under the control of the organization.

Upon request, the organization must,

- **Correct** the information as soon as **reasonably possible**; and
- Where the organization has disclosed the incorrect information to other organization, **send a notification** containing the corrected information, **if it reasonable to do so**.

If an organization does not make the correction, it must **annotate** the personal information under its control with the correction that was requested but not made. However, an organization **must** correct information disclosed to other organizations in its custody or under its control.

Duty to Assist

An organization must make every **reasonable effort** to assist applicants, and to respond to each applicant as accurately and completely as reasonably possible, and, if it is reasonable to do so, explain any term, code or abbreviation used in any record.

An organization must also create a record for the applicant if

- The record can be created from a record that is in electronic form and that is under the control of the organization, using its normal computer hardware and software and technical expertise; and
- Creating the record would not unreasonably interfere with the operations of the organization.

Time Limit for Responding

An organization must respond to an applicant not later than **45 days** from the day that the organization receives the applicant's written request, or the end of an extend time period if extended (see below).

Failure to respond to a request is to be treated as a decision to **refuse** the request.

Contents of Response

In a response to a request for **access to records**, the organization **must** inform the applicant:

- As to whether or not the applicant is entitled to or will be given access;
- When access will be given (if permitted);
- If access is refused,
 - The reasons and provisions on which the refusal is based;
 - Name of person who can answer on behalf of the organization; and
 - That the applicant may ask for review under section 46.

In a response to a request to provide information about **use of disclosure of information**, the organization **must**:

- Provide the applicant with
 - Information about the purposes for which the personal information has been and is being used by the organization; and
 - The names of the persons to whom and circumstances which the person information has been and is being disclosed.

or

- If the organizations refuses, inform the applicant of
 - The name of the person who can answer on behalf of the organization; and
 - That the applicant may ask for review under section 46.

In response to a request for correction, the organization must inform the applicant:

- Of any action taken in response to the request;
- The name of the person who can answer on behalf of the organization; and
- That the applicant may ask for a review under section 46.

How Access Will Be Given

Where an applicant is informed that access to the personal information will be given, the organization **must**:

- If the applicant has asked for a copy of the applicant's personal information and the information can reasonably be reproduced,
 - Provide with the response a copy of the record or the part of the record containing the information; or
 - Give the applicant reasons for the delay in providing the information or record.

or

- If the applicant has asked to examine the record containing the applicant's personal information or the record cannot be reasonably be reproduced,
 - Permit the applicant to examine the record or part of the record; or
 - Give the applicant access in accordance with the regulations.

Extending the Time Limit for Responding

An organization may extend **30 days** or, with the Commissioner's permission, to a longer period, if:

- The applicant doesn't give sufficient detail;
- A large amount of information is requested;
- Meeting the time limit would unreasonably interfere with operations; or
- More time is needed to consult with another business.

If extended, the organization must inform the applicant of the following:

- The reason for the extension;
- The time when a response can be expected; and
- That the applicant may ask for review under section 46.

Fees

An organization **may** charge a **reasonable fee** for access to the applicant's personal information or information about the use or disclosure of same. The organization **must** give the applicant a written estimate of the total fee and may require the applicant to pay a deposit.

An organization **may not** charge a fee for a request for correction or a request for personal employee information.

Care of Personal Information

Accuracy of Information

An organization must make a **reasonable** effort to ensure that any personal information collected, used or disclosed is accurate and complete to the extent **reasonable**.

Protection of Information

An organization must protect personal information that is in its custody or under its control by making **reasonable** security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

Notification of Loss or Unauthorized Access or Disclosure

An organization having personal information under its control **must**, without **unreasonable delay**, provide notice to **the Commissioner** of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a **real risk of significant harm** to an individual as a result of the loss, unauthorized access or disclosure.

Retention and Destruction of Information

An organization may retain personal information only for as long as the organization **reasonably** requires the information for legal or business purposes.

Within a reasonable period of time thereafter, the organization must:

- Destroy the records; or
- Render the personal information non-identifying so that it can no longer be used.

Enforcement

Protection of Organization from Legal Action

No action lies and no proceeding may be brought against an organization, or any person acting on behalf of or under the direction of an organization, for damages resulting from:

- The disclosure of or failure to disclose, in good faith, all or part of a record or personal information under this Act, or any consequences of that disclosure or failure to disclose, or
- The failure to give a notice required under this Act if reasonable care was taken to give the required notice.

Offenses

A person who that commits an offense may be subject to a fine of not more than \$100,000. Offenses include, among other things, collecting, using and disclosing personal information in contravention of the Act, disposing of personal information to evade an access request, obstructing the Commissioner, and failing to comply with an order.

C. British Columbia's Personal Information Protection Act

Personal Information Protection Act, S.B.C. 2003, c. 63 (Can.)

Purpose

The purpose of the British Columbia Personal Information Protection Act ("BCPIPA") is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of the individuals to protect their personal information and the need of organizations to collect, use or disclosure personal information for purposes that a reasonable person would consider appropriate in the circumstances.

Application

The BCPIPA applies to every organization collecting, using, or disclosing personal information.

What is personal information?

"Personal information" means information about an identifiable individual and includes employee persona information but does not include: contact information or work product information.

General Rules Respecting Protection of Personal Information by Organizations

Compliance

An organization must consider what a **reasonable person** would consider appropriate in the circumstances.

- An organization is responsible for personal information under its control, including personal information that is not in the custody of the organization;
- **Security Compliance Officer:** An organization must designate one or more individuals to be responsible for ensuring that the organization complies with this Act;

- An individual designate one or more individuals to be responsible for ensuring that the organization complies with this Act;
- An organization must make available to the public;
 - The **safety compliance officer(s)**;
 - **Contact** information for same.

Policies and Practices

An organization **must**:

- Develop and follow policies and practices;
- Develop a process to respond to complaints;
- Make information available on request about:
 - Policies and practices; and
 - The complaint process.

Consent

Consent Required

An organization must **not** collect, use, or disclose personal information about an individual, unless the individual:

- Gives consent;
- The BCPIPA authorizes the collection, use or disclosure **without** consent;
- The BCPIPA deems the collection, use or disclosure to be consented to by the individual.

Implicit Consent

An individual is deemed to consent to the collection, use or disclosure of personal information if:

- The purpose would be considered to be obvious to a reasonable person; and
- The individual voluntarily provides the personal information.

An organization may collect, use or disclose personal information about an individual for specified purposes if:

- The organization provides the individual with notice that it intends to collect, use or disclose the individual's personal information for those purposes;
- The organization gives the individual a reasonable opportunity to decline within a reasonable amount of time;
- The individual does not decline, within the time allowed;
- The collection, use or disclosure is reasonable with regard to the sensitivity of the information.

Withdrawal of Consent

On giving reasonable notice, an individual **may** withdraw consent to the collection, use or disclosure of personal information about the individual at any time. An organization must thereafter inform the individual of the likely consequences of the withdrawal.

An individual **may not** withdraw consent if it would frustrate the performance of a legal obligation.

Collection of Personal Information

Required Notification

On or before collecting personal information, an organization **must** disclose to the individual **verbally or in writing**:

- The **purpose** of the collection; and
- On request of the individual, the position name or title and contact information of the **Security Compliance Officer(s)**.

On or before collecting personal information about an individual from another organization without consent, an organization must provide the other organization with sufficient information regarding the purpose of the collection to determine whether the disclosure is sufficient under the BCPIPA.

Limitations on Collection of Personal Information

An organization may collect personal information only for the purpose that a **reasonable** person **would consider appropriate** in the circumstances and that fulfill the purposes that the organization discloses in the notification to the individual and otherwise permitted under the BCPIPA.

Collection of Personal Information without Consent

An organization may collect personal information about an individual without consent or from a source other than the individual if (irrelevant exceptions omitted):

- The collection is **clearly** in the interest of the individual and consent cannot be obtained in a **timely** way;
- **Medical:** The collection is necessary for the medical treatment of the individual and the individual is unable to consent;
- **Investigation or Proceeding:** It is reasonable to expect the collection with the consent of the individual would compromise the availability or the accuracy of the personal information and the collection is reasonable for an investigation or proceeding.

An organization may collect personal information from or on behalf of another organization without consent of the individual if:

- The individual previously consented to the collection by the other organization; and
- The personal information is disclosed to or collected by the organization solely
 - For the purpose for which the information was previous collected; and
 - To assist that organization to carry out work on behalf of the organization.

Collection of Employee Personal Information

An organization **may** collect employee personal information without consent of the individual.

An organization **must** notify an individual that it will be collecting personal information about the individual and the purpose for the collection prior to collecting the information without consent.

Use of Personal Information

Limitations on Use of Personal Information

An organization may use personal information only for purposes that are reasonable person would consider appropriate under the circumstances.

Use of Personal information without Consent

An organization may use personal information about an individual without consent of the individual, if (irrelevant exceptions omitted)

- The use is **clearly** in the interest of the individual and consent cannot be obtained in a **timely** way;
- **Medical:** the use is necessary for the medical treatment of the individual and the individual does not have the legal capacity to give consent;

- **Legal:** it is reasonable to expect that the use with the consent of the individual would compromise an investigation or proceeding and the use is reasonable for purposes related to an investigation or proceeding;
- **Emergency:** the use is necessary to respond to an emergency that threatens the life, health, or security of an individual.

An organization may use personal information from or on behalf of another organization without consent of the individual if:

- The individual previously consented to the use by the other organization; and
- The personal information is used by the organization solely;
 - For the purpose for which the information was previous collected; and
 - To assist that organization to carry out work on behalf of the organization.

Disclosure of Personal Information

Limitations on Disclosure of Personal Information

An organization may disclose personal information only for purposes that a reasonable person would consider appropriate under the circumstances.

Disclosure of Personal Information Without Consent

An organization may **only** disclose personal information without consent if:

- The disclosure is **clearly** in the interest of the individual and consent cannot be obtained in a **timely** way;
- **Medical:** the disclosure is necessary for the medical treatment of the individual and the individual does not have the legal capacity to give consent;
- **Legal:** it is reasonable to expect that the use with the consent of the individual would compromise an investigation or proceeding and the use is reasonable for purposes related to an investigation or proceeding;
- **Court Order/Subpoena:** the disclosure is for the purpose of complying with a subpoena, warrant, or court order, person or body with jurisdiction to compel the production;
- **Health/Safety:** There are reasonable grounds to believe that compelling circumstances exist that affect the health or safety of any individual and if notice of disclosure is mailed to the last known address of the individual to whom the personal information relates;

- **Death:** The disclosure is for the purpose of contacting next of kin or a friend of an injured, ill or deceased individual;
- The disclosure is to a lawyer who is representing the organization.

An organization may disclose personal information to another organization without consent of the individual to whom the information relates, if

- The individual consented to the collection of the personal information; and
- The personal information is disclosed to the other organization solely for the purpose for which the information was previous collected and to assist the other organization to carry out work on behalf of the organization.

Disclosure of Employee Personal Information

An organization may disclose personal information without the consent of the individual.

An organization **must** notify an individual that it will be disclosing employee personal information about the individual and the purposes for the disclosure before the organization discloses the information.

Access to and Correction of Personal Information

Access to Personal Information

On request of an individual, an organization must provide the individual with the following:

- The individual's personal information under the control of the organization;
- Information about the ways in which the information was used;
- The names of the individuals and organizations to whom the information was disclosed.

An organization **must not** disclose personal information and other information if:

- The disclosure could reasonably be expected to threaten the safety or physical or mental health of an individual other than the individual who made the request;
- The disclosure can reasonably be expected to cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;
- The disclosure would reveal personal information about another individual;
- The disclosure would reveal the identity of an individual who has provided personal information about another individual and the individual providing the personal information does not consent to disclosure of his or her identity.

Right to Request Correction of Personal Information

An individual may request an organization to correct an error or omission in the personal information that is:

- About the individual; and
- Under the control of the organization.

If the organization is satisfied on reasonable grounds that a request should be implemented, the organization must:

- Correct the personal information as soon **as reasonably possible**; and
- Send the corrected personal information to each organization to which the personal information was disclosed by the organization during the year before the date the correction was made.

Administration

Duty to Assist

An organization must make a reasonable effort:

- To assist each applicant;
- To respond to each applicant as accurately and completely as reasonably possible; and
- To provide each applicant with the requested information or with a reasonable opportunity to examine the information if the request cannot be reasonably provided.

Time Limit for Response

An organization **must** respond to an applicant not later than **30 days** after receiving the applicant's request or the end of an **extended time** provided below.

Content of Response

If access to all or part of the personal information requested by the applicant is refused, the organization must tell the applicant:

- The reasons for the refusal and the provision of the BCPIPA on which the refusal is based;
- The name of the person and title who can answer questions on behalf of the organization;
- That the applicant may ask for review within 30 days.

Extending the Time Limit for Response

An organization **may extend** the time for responding for up to an additional **30 days** or, with the Commissioner's permission, for a longer period if:

- The applicant does not give enough detail to enable the organization to identify the personal information requested;
- A large amount of information is requested or must be searched which would interfere with the operations of the business; or
- More time is needed to consult with another organization to decide whether to allow access.

If time **is extended**, the organization must tell the applicant:

- The reason for the extension;
- The time when a response from the organization can be expected; and
- The rights of the applicant to complain about the extension and request that an order be made.

Fees

An organization **must not** charge an individual a fee respecting employee information.

An organization **may** charge an individual who makes a request for access a minimal fee that is not an employee. The organization must give the applicant a **written estimate**, and may require the applicant pay a **deposit** of all or part of the fee.

Care of Personal Information

Accuracy of Personal Information

An organization **must** make a reasonable effort to ensure that personal information collected is **accurate and complete**, if the information:

- Is likely to be used by the organization to make a decision about the individual; or
- Is likely to be disclosed by the organization to another organization.

Protection of Personal Information

An organization must protect personal information in its custody or under its control by making **reasonable security arrangements** to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar acts.

Retention of Personal Information

If an organization uses an individual's personal information to make a decision that directly affects the individual, the organization must retain that information for **at least one year** after using it so that the individual has a **reasonable opportunity** to obtain access to it.

An organization **must destroy** its documents containing personal information, or remove the means by which they can be associated, as soon as it is reasonable to assume that:

- The purpose is no longer being served by retention;
- Retention is no longer necessary for legal or business purposes.

Enforcement

A person who that commits an offense may be subject to a fine of not more than \$100,000. Offenses include, among other things, disposing of personal information to evade an access request, obstructing the Commissioner, and failing to comply with an order.

D. Quebec's Act Respecting the Protection of Personal Information in the Private Sector.

Act Respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1 (Quebec)

The object of the Quebec Act Respecting the Protection of Personal Information in the Private Sector ("Quebec Privacy Act") is to establish particular rules with respect to personal information relating to other persons which a person collects, holds, uses or communicates to third persons in the course of carrying on an enterprise.

What is personal information?

"Personal information" is any information which relates to a natural person and allow that person to be identified.

Collection of Personal Information

Any person collecting personal information to establish a file on another person or to record personal information in such a file may collect **only the information necessary** for the object of the file. Such information **must** be collected by a lawful means.

A person who collects personal information from the person concerned **must**, when establishing a file on that person, **inform him**:

- Of the object of the file;

- Of the use which will be made of the information and the categories of persons who will have access to it;
- Of the place where the file will be kept and of the rights of access and rectification.

Confidentiality of Personal Information

Retention, Use and Non-communication of Information

Policies & Procedures: A person carrying on an enterprise **must** take the security measures necessary to ensure protection of the personal information that are **reasonable** given:

- The sensitivity of the information;
- The purpose for which it is to be used;
- The quantity and distribution of the information; and
- The medium on which it is stored.

Accuracy: Every person carrying on an enterprise must ensure that any file held on another person is **up to date** and **accurate** when used to make a decision in relation to the person concerned.

Objective/Purpose Complete: Once the object of the file has been achieved, no information contained in it may be used otherwise than with the consent of the person concerned.

Third-Party: No person may communicate to a third person the information on another person, or use it for purposes not relevant, unless the person consents or use is provided by the Act.

Consent: Consent to the collection, communication or use of personal information **must** be manifest, free, and enlightened, and must be given for specific purpose. Consent is valid only for the length of time necessary to achieve the purpose.

Communication to Third Persons

A person carrying on an enterprise may, without the consent of the person concerned, communicate personal information contained in a file he holds on that person (inapplicable exceptions omitted):

- To his attorney;
- To a person whom the information must be communicated by reason of the urgency of a situation that threatens the life, health or safety of the person concerned.

Cross-Border Transfer: Every person who communicates personal information outside of Quebec or entrusts a person outside of Quebec with the task of holding, using or communicating such information **must first** take all reasonable steps to ensure:

- The information will not be used for purposes not relevant to the object of the file or communicated to third persons without consent (with the certain exceptions above)

Access by Persons Concerned

General Provisions

Access: Every person carrying on an enterprise who holds a file on a person **must**, at the request of the person concerned, **confirm the existence** of the file and communicate to the person any personal information concerning him.

Deletion: In addition, the person concerned is entitled to obtain that any personal information collected be **deleted**.

An organization must take the necessary steps to ensure the exercise by a person concerned of the rights provided by this Act. In particular, they must inform the public of the place where, and manner in which, access to the files may be granted.

Procedure

Procedure for Access: Access or rectification may **only be considered** if **in writing** by a person who proves that he is the person concerned or the representative of the person concerned.

Response: an organization must respond **not later than 30 days** after the receipt of the request, and access shall be **free of charge** (unless a transcription, reproduction or transmission is requested).

Refusal: A refusal must inform:

- In writing;
- Giving reasons; and
- Inform the person concerned of the recourses open to him.

Restrictions on Access

Third Person: An organization **must** refuse access where:

- Disclosure would be likely to reveal personal information about a third person; or
- The existence of such information and the disclosure may seriously harm that third person, unless the latter consents to the communication or in a case of emergency.

Enforcement

Every organization who collects, holds, communicates to third persons or uses personal information on other persons otherwise than in accordance with the provisions of the Privacy Act is liable to a fine of \$1,000 to \$10,000 and, for a subsequent offence, to a fine of \$10,000 to \$20,000. For a contravention of section 17 (cross-border transfer), the fine is \$5,000 to \$50,000 and, for a subsequent offence, \$10,000 to \$100,000.

E. Canada's Anti-Spam Legislation

Canadian Anti-Spam Law, *S.C. 2010, c. 23*, §11 (Can. 2010)

Canada's Anti-Spam Legislation ("CASL") establishes rules for the sending of commercial electronic messages⁹⁶ ("CEM") and the installation of computer programs.

Commercial Electronic Messages

A CEM is an electronic message that it would be reasonable to conclude has as its purpose to encourage participation in a commercial activity⁹⁷, including an electronic message that:

- (a) Offers to purchase, sell, barter or lease a product, goods, a service, land or an interest or right in land;
- (b) Offers to provide a business, investment or gaming opportunity;
- (c) Advertises or promotes anything referred to in paragraph (a) or (b); or
- (d) Promotes a person, including the public image of a person, as being a person who does anything referred to in any of paragraphs (a) to (c), or who intends to do so.

CASL 2. An electronic message that contains a request for consent to send a message described above is also considered to be a commercial electronic message. CASL 3. However, an electronic message described above that is sent for the purpose of law enforcement, public safety, the protection of Canada, the conduct of international affairs or the defense of Canada is **not** considered to be a commercial electronic message. CASL 4.

Requirements and Prohibitions

Unsolicited Electronic Messages

It is prohibited to send or cause or permit to be sent to an electronic address a commercial electronic message unless:

⁹⁶ An "electronic message" means "a message sent by any means of telecommunication, including a text, sound, voice or image message. CASL 1.

⁹⁷ A "commercial activity" means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, whether or not the person who carries it out does so in the expectation of profit, other than any transaction, act or conduct that is carried out for the purposes of law enforcement, public safety, the protection of Canada, the conduct of international affairs or the defense of Canada." CASL 1.

- The recipient of the message has consented (express or implied);
- The message identifies the person who sent the message and the person – if different – on whose behalf it is sent (information must be valid for a minimum of 60 days after the message was sent, CASL 6(3));
 - Sets out information to readily contact one of the persons who sent the message; and
 - Sets out an unsubscribe mechanism.

CASL 6(1)–(2).

Exceptions

This provision does not apply to the following:

- That is sent by or on behalf of an individual with whom they have a personal or family relationship, as defined by the regulations;
- That is sent to a person who is engaged in a commercial activity and consists solely of an inquiry or application related to that activity; or
- That is of a class, or is sent in circumstances, specified by the regulations.

CASL 6(5)(a)–(c).

Additionally, **consent** is not required for a CEM that solely:

- **Quote**: Provides a quote or estimate for the supply of a product, goods, or service if requested by the person to whom the message is sent.
- **Commercial Transaction**: Facilitates, completes, or confirms a commercial transaction that the recipient previously agreed.
- **Warranty/Recall**: Provides warrant information, product recall information, or safety or security information about a product, good, or service that the person uses, has used, or has purchased.
- **Factual Information**: Provides factual information about:
 - the ongoing use or ongoing purchase by the person to whom the message is sent of a product, goods, or service offered under a subscription, membership, account, loan or similar relationship by the person who sent the message or on behalf thereof; or
 - the ongoing subscription, membership, account, loan or similar relationship of the person to whom the message is sent.

- **Employment Relationship**: Information directly related to an employment relationship or related benefit plan in which the person to whom the message is sent is currently involved.
- **Delivery**: Delivers a product, good or service, including product updates or upgrades, that the person to whom the message is sent is entitled to receive under the terms of the transaction that they have previously entered into with the person who sent the message.
- **Regulations**: Communications for a purpose specified by the regulations.

This Provision also does not apply to a commercial electronic message that is:

- An interactive two-way voice communication between individuals;
- Sent by means of facsimile to a telephone account; or
- A voice recording sent to a telephone account.

CASL 6(8)(a)–(c).

Consent

Express consent

- A person who seeks express consent for sending commercial electronic messages, when requesting consent, must set out clearly and simply the following information:
 - The purpose or purposes for which the consent is being sought;
 - Prescribed information that identifies the person seeking consent and, if the person is seeking consent on behalf of another person, prescribed information that identifies that other person; and
 - Any other proscribed information.

CASL 10(1)(a)–(c).

If the individual is unknown:

- The only information that is required is prescribed information that identifies the person seeking consent; and
- The person seeking consent must comply with the regulations in respect of the use that may be made of the consent and conditions on which the consent may be used.

CASL 10(2)(a)–(b).

Implied consent

- Consent is implied only if:
 - **Existing Business Relationship:** The person who sends the message, the person who causes it to be sent or the person who permits it to be sent has an existing business relationship or an existing non-business relationship with the person to whom it is sent;
 - **Knowing Disclosure:** The person to whom the message is sent has conspicuously published, or has caused to be conspicuously published, the electronic address to which the message is sent, the publication is not accompanied by a statement that the person does not wish to receive unsolicited commercial electronic messages at the electronic address and the message is relevant to the person's business, role, function or duties in a business or official capacity;
 - The person to whom the message is sent has disclosed, to the person who sends the message, the person who causes it to be sent or the person who permits it to be sent, the electronic address to which the message is sent without indicating a wish not to receive unsolicited commercial messages at the electronic address, and the message is relevant to the person's business, role, functions or duties in a business or official capacity; or
 - The message is sent in the circumstances set out in the regulations.

CASL 10(9)(a)–(d).

An “existing business relationship” means a business relationship between the person to whom the message is sent arising from

- the purchase or lease of a product, goods, a service, land or an interest or right in land, within the **two-year period immediately before the day on which the message was sent, by the person to whom the message is sent from any of those other persons;**
- an inquiry or application, **within the six-month period immediately before the day on which the message was sent.**

CASL 10(10)(a) and (3) (emphasis added).

Unsubscribe

The unsubscribe mechanism must enable the person to whom the commercial electronic message is sent to indicate, at no cost to them, the wish to no longer receive any commercial electronic messages, or any specified class of such messages, from the person who sent the message, using: (i) the same electronic means by which the message was sent, or (2) if using those means is not practicable, any other electronic means that will enable the person

to indicate the wish, and (3) specify an electronic address, or link to a page on the World Wide Web that can be accessed through a web browser, to which the indication may be sent. CASL 11(1).

The person who sends the commercial electronic message must ensure that the electronic address of World Wide Web page is valid for a minimum of 60 days after the message has been sent. CASL 11(2). The person who sent the commercial electronic message must ensure that effect is given to an indication regarding unsubscribing without delay, and in any event no later than 10 business days after the indication has been sent, without any further action being required on the part of the person who so indicated.

Violations

The maximum penalty for a violation is \$1,000,000 in the case of an individual, and \$10,000,000 in the case of any other person.

XV. Cape Verde

Data Protection Law, 133/V (2001), as amended by Law 41/VIII (2013), Law 132/V (2001)

The Data Protection Law (“DPA”) governs the collections and processing of personal information in Cape Verde.

Personal Information

Personal information is defined as any information, regardless of its nature or the media on which it is stored, relating to an identifiable natural person. Sensitive data is defined as:

- Philosophical or political convictions;
- Party or union affiliations;
- Religious faith;
- Private life;
- Ethnic origin;
- Health;
- Sex life;
- Genetic information.

Registration

A company must register with the data protection authority (comissao nacional de protecao de dados pessoais) prior processing data.

Data Protection Officers

Not required by the DPA.

Collection and Processing of Personal Information

Personal information must be:

- Processed lawfully and in good faith;
- For specific, explicit and legitimate purpose;
- Adequate, relevant, and not excessive;
- Accurate;
- Not kept longer than necessary.

The processing of sensitive personal information requires expressed consent with adequate measures of assurance.

Transfer of Personal Information

The DPL permits international transfer of personal data only if the recipient country is considered to have a sufficient level of protection, which is defined by the data protection authority.

Security of Personal Information

The DPL requires a company to implement technical and organizational measures to ensure the confidentiality and security of the personal information processed. These obligations must also be contractually enforced by the company and, if applicable, the data processor.

Breach Notification

Not required by the DPL.

Enforcement

Any person who suffers as a result of any inappropriate use of personal information has the right to bring a civil claim against a company. Violations of the DPL are punishable with a term of imprisonment of up to two years or a fine of up to 240 days. Additional sanctions may be imposed, such as: temporary or permanent prohibition on processing data, advertisement of a sentence, or a public warning.

XVI. Chile

Data Protection Act, Law No. 19628 (1999), proposed amendment (2018)

The treatment of personal information in public and private databases is governed in Chile by Law 19,628 “On the protection of life,” commonly referred as “Personal Data Protection Law” (“PDPL”).

Personal Information

Personal information is defined as any information concerning natural persons, whether identified or identifiable.

Sensitive personal information relates to the physical or moral characteristics of persons, or facts or circumstances of their private life or intimacy, such as personal habits, racial origin, political ideologies and opinions, religious creed or beliefs, physical and mental health conditions, and sexual life.

Data Protection Officer

According to the PDPL, the company is responsible for ensuring that personal data is protected in accordance with applicable legal requirements. The responsible person must also respond to inquiries of any person regarding his or her personal data, and its modification, deletion or blocking. If no answer is provided, the individual may initiate a civil procedure before the corresponding authorities.

Collection & Processing of Personal Information

The PDPL establishes conditions under which personal data shall be “treated.” Treatment is defined to include “any operation or set of operations, whether automated or not, that recalls, displays accesses, saves, records, organizes, elaborates, selects, extracts, confront, interconnects, dissociates, communicates, deletes, transfers, transmits or cancels personal data, or the use of personal data in any other form or manner.”

As a general rule, persona data can only be “treated” when the written consent of the owner of the persona data is obtained, or when one of the following is met:

- Authorization by law;
- Collection from publicly accessible sources;
- The data is economic, financial, banking or commercial nature, provided the further treatment of this information meets a number of specific requirements;
- When personal data is treated by private entities solely for their, or their associate and affiliated entities’ exclusive internal use.

Security of Personal Information

All personnel involved in treatment of personal data have a legal obligation of confidentiality. The company must keep data “with due diligence, being held accountable for damages.

Breach Notification

No obligation to provide breach notification.

Enforcement

No criminal sanctions (imprisonment and fines) for breaching information treatment systems and/or revealing any information contained therein.

Amendment

On April 3, 2018, the Chilean Senate voted to approve for consideration an amendment to the Data Protection Act No. 19,628. The amendment delves into the rights of data subjects, taking into account the high standards imposed by the EU with regard to this matter.

XVII. China

PRC Cybersecurity Law, Arts 1-79 (2017)

In 2017, the People’s Republic of China (“PRC”) adopted the PRC Cybersecurity Law (“PRC CL”). On December 29, 2017, the PRC also issued the Information Security Techniques – Personal Information Security Specification (“PI Standards”) which outlines certain requirements for the collection, use, and storage of personal information.

Personal Information

According to the PRC CL, Personal information refers to all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person’s identity, including but not limited to natural persons’ full names, birth dates, national identification numbers, personal biometric information, addresses, telephone numbers, and so forth.

According to the PI Standards, sensitive personal information is defined as the leakage, illegal provision or abuse of which may harm personal/property safety and personal reputation or physical/mental health, or result in discrimination towards the individual. The PRC CL, however, does not make a distinction between personal information and sensitive personal information.

Data Protection Officers

The PRC CL does not require a data protection officer. However, the PI Standards require that an institution or personnel be appointed if: (1) the primary business of an organization is related to data processing and there are more than 200 employees; (2) personal data of more than 500,000 individuals are processed; or personal data of more than 500,000 individuals is expected to be processed within twelve months.

Collecting and Processing of Personal Information

Clear consent is required.

Under the PRC CL, a company may collect and use personal information if the following conditions are met:

- Abide by the principles of legality, legitimacy and necessity, and may not be excessive;
- Explicitly notify the purposes, means and scope of collection, use and disclosure of personal information;
- Obtain the data subject's clear consent to the personal information collection, use and disclosure;
- Not violate laws, regulations or agreements between the company and the data subject when collecting or using the personal information; and
- Make publicly available the company's rules or policy regarding the collection and use of personal information.

The PI Standards imposes additional burdens on a corporation, and require the following in the privacy policy:

- The identity of the company, including registered names, registered address, principal office, a telephone number and/or email address;
- The list of personal data information collected for each business purpose, processing policies including location of storage, retention, period, frequency of collection, etc.;
- The purposes sought by the company;
- The circumstances under which the information may be shared, assigned, or transferred;
- The basic data security principles, as well as the data protection measures to be adopted;
- The right to access, rectify, delete, de-register, withdraw consent, and to obtain copies of their personal information;
- Potential risks of providing personal information, as well as the impact on not providing personal information;
- Channels and mechanisms for making inquiries or lodging complaints.

The information in the data protection policy must be true, accurate, and complete. The contents must be clear and easy to understand, follow common language habits, use standard numbers and graphics for illustration, and ambiguous language should be avoided. Also, an abstract should be

provided at the beginning of the policy, and the policy should be published publicly and easily accessible. Data subjects should be notified of any changes to the policy.

Transfer of Personal Information

The PRC CL prohibits the disclosure or transfer of an individual's personal information to others without the individual's consent.

Security of Personal Information

A company must take appropriate technical and organizational measures against unauthorized or unlawful processing and against accidental loss, destruction of, or damage to, personal information. Under the PRC CL, a company is required to establish information protection systems. The system must ensure the security of personal information and to prevent the collected data from being accidentally disclosed, tampered with or destroyed.

Breach Notification of Personal Information

The PRC CL requires a company to “promptly take relevant measures to prevent the aggravation of the damages and promptly notify relevant data subjects and report to relevant government agencies in accordance with relevant provisions.” This requirement is without specific or clear guidance on the timeline for reporting and without identifying which agency is in charge.

On the other hand, the PI Standards provide the following:

Contingency Response and Reporting of Security Incidents

- A contingency plan for security incidents of personal data should be formulated;
- Organize trainings of contingency response and contingency drills regularly (once a year), in order to let relevant internal staff understand their responsibilities, strategies and procedures for contingency response;
- When a data breach/security incident occurs, the following actions should be taken:
 - Record the content of the incident, including but not limited to: the person who discovers the incident, the date, the place, personal data and number of people involved in the incident, the name of the system in which the incident occurs, impact on other interconnected systems, whether the law enforcement department or other relevant department have been contacted;
 - Assess the possible impact of the incident, and take necessary measures to control the situation and eliminate potential dangers;
 - If applicable, report to the relevant government agency in accordance with the “National Network Security Incident Contingency Response Plan”, the content of the report shall include but not limited to: general information such as the type, number, content and nature of the data subjects involved, potential impact of the

incident, measures taken or to be taken, contact details of relevant persons involved with handling the incident; and

- Update the contingency response plan in a timely manner pursuant to the changes of relevant laws and regulations as well as the situation of the incident.

Notification of Security Incidents

- Notify data subjects of relevant information of the incident by mail, letter, telephone, push notification or other means in a timely manner. If it is hard to notify each data subject, organizations shall take reasonable and effective measures to publish warning message relevant to the public;
- The content of the notification shall include but not limited to:
 - The content and impact of the security incident;
 - The measures taken or to be taken;
 - Suggestions for data subjects regarding how to take initiative to prevent and reduce the risk of security incidents;
 - Remedies specifically provided for data subjects; and
 - Contact persons and organizations responsible for personal data protection.

Enforcement

The PRC CL allows for corrections, warnings, confiscation of illegal gains and fines of up to 10 times of illegal gains (or fines of up to RMB 1,000,000 where there is no illegal gain) upon discovery of a violation in handling personal information. The responsible person may also be fined between RMB 10,000 to 100,000.

XVIII. Costa Rica

Undisclosed Information Law, No. 7975 (2000)

Protection in the Handling of the Personal Data of Individuals, No.8968 (2011)

The collection and processing of personal information in Costa Rica is divided among two laws – Law No. 7975 (Undisclosed Information Law) and Law No. 8968 (Protection in the Handling of the Personal Data of Individuals) (hereinafter the “Laws”).

Personal Information

Personal information is information contained in public or private registries that identifies or could be used to identify a natural person. Sensitive personal information is information

revealing racial origin, political opinions, religious or spiritual beliefs, socioeconomic status, genetic information, or sexual orientation.

Registration

All databases, public and private, administered for the purposes of distribution, disclosure, or business administration must register with the Agencia de Proteccion de Datos de los habitantes (“Agency”).

Data Protection Officer

Not required by the Laws.

Collection and Processing of Personal Information

In order to collect personal data, a data controller must obtain written (physical or electronic) consent from the data subject after informing the data subject of:

- The existence of the database;
- The purpose of the collection;
- The destination of the information;
- Who can review the information;
- Whether collection is optional;
- The consequences of refusal;
- The ability to exercise certain rights; and
- The identity and address of the company.

Consent is not required by law or where the data is obtained from public sources.

No person can be required to provide sensitive persona information, unless:

- The data processing is carried out during the course of the legitimate activities of a foundation, association, or other body with a political, philosophical, religious, or trade union purpose, and the data solely relates to members or people who have regular contact with the organization.
- The processing is to protect the vital interests of another person or, in the event that the person concerned is incapable of consent;
- The processing relates to data that the person concerned has released voluntarily;

- The processing is necessary for the establishment, exercise, or defense of a right in a judicial proceeding; or
- The processing is necessary to the provision of medical care and performed by someone with an obligation to keep the data confidential.

Transfer of Personal Information

A company may only transfer data when the individual consented explicitly and validly to the transfer and such transfer was made without violating the principles and obligations under the law. Data managers must establish a contract with data transferors to ensure the transferor is held to at least the same standards as the data manager.

Security of Personal Information

A company must take such technical and organizational measures as are necessary to guarantee the security of personal information in order to avoid their alteration, loss, and unauthorized access. The regulations establish certain minimum protocols that must be implemented and registered with the Agency:

- Developing policies and manuals concerning data privacy and protection;
- Implementing a training manual and procedure regarding staff awareness on the protection of personal information;
- Establishing procedures to respond to complaints and questions, as well as requests to access, amend, modify, block, or delete a data owners data or to revoke consent for processing;
- Creating measures and technical procedures to maintain a record of personal information during processing; and
- Establishing procedures to inform any transferors of data of the data security obligations required.

The specific security measures taken shall consider the following factors:

- The sensitivity of the personal data processed;
- The technology used for processing;
- Potential consequences of a violation of privacy in the data;
- Previous vulnerabilities; and
- Any other factors that may be applicable.

Breach Notification

A company must inform an individual of irregularities in the processing of storage of data, such as loss, destruction, or theft due to a security vulnerability. A company must notify the affected party within five days of the incident, and also conduct a thorough review within that time frame. Finally, a company must notify the Agency of the incident (no specific timeline).

Any notice provided must contain information regarding:

- The nature of the incident;
- The personal data compromised;
- The corrective actions that have been taken; and
- Instructions for obtaining further information about the incident.

Enforcement

A private citizen may bring a suit in court where their rights to privacy or data protection have been violated. Criminal prosecutors may also bring actions on behalf of individuals for the misuse of intimate or private data, a crime punishable by up to three years imprisonment if the defendant is responsible for the data. A company is also subject to fines ranging from fifteen to thirty base salaries and a suspension from database use of up to six months.

XIX. Croatia

See GDPR discussion.

XX. Cyprus

See GDPR discussion.

XXI. Czech Republic

See GDPR discussion.

XXII. Denmark

Danish Act on Data Protection, Act No. 502 of 23 (2018)

Denmark is regulated by the GDPR with supplemental provisions provided by the Danish Act on Data Protection (“Act”). The supplements from the Act will be summarized below.

Personal Information

Personal “data” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by

reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. In Denmark, information relating to a deceased person is considered personal data as well until 10 years after perishing.

Registration

In Denmark, the following types of processing requires the Datatilsynet (“DPA”) preapproval:

- Private data controllers’ processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation’

Data Protection Officer/Collection and Processing/Transfer/Security

See GDPR discussion.

Enforcement

In addition to GDPR sanctions, any person suffering material or nonmaterial damage due to non-legal data processing can claim damages. Unless a higher penalty is impeded, processing deemed unlawful under the Act, is sanctioned with a fine or prison for up to six months.

XXIII. Estonia

See GDPR discussion.

XXIV. Finland

See GDPR discussion.

XXV. France

See GDPR discussion.

XXVI. Germany

See GDPR discussion.

XXVII. Greece

See GDPR discussion.

XXVIII. Hong Kong

Personal Data Privacy Ordinance, HKO Cap.486 s.11 (1996)

The Personal Data (Privacy) Ordinance (Cap. 486) (“Ordinance”) regulates the collection and handling of personal data.

Personal Information

Personal “data” is defined in the Ordinance as any 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; and
- In a form in which access to or processing of data is practicable.

Data Protection Officers

Not required under the Ordinance.

Collection and Processing of Personal Information

A company may collect data if:

- The personal data is collected for a lawful purpose directly related to a function or activity of the data user;
- The collection is necessary for or directly related to that purpose;
- The data to be collected is adequate but not excessive; and
- All practical steps have been taken to ensure that the data subject has been informed, on or before collection of the data, of the following:
 - Whether the supply of personal data by the data subject is obligatory or voluntary and, if obligatory, the consequences of not supplying the data;
 - The purpose for which the data will be used;
 - The person to whom it may be transferred;
 - Right of access or correction;
 - The name or job title, and address, of the individual requests should be sent.

Transfer of Personal Information

A company may not transfer to a third-party unless the individual has been informed on or before the individual's information was collected:

- That his/her personal information may be transferred; and
- The classes of persons to whom the data may be transferred.

The ordinance does not discuss outside of Hong Kong transfers.

Security of Personal Information

A company must take all practicable steps to ensure that personal information is protected against unauthorized or accidental access, processing, erasure, loss or use, having regard to factors including the nature of the personal information and the harm that could result if data breaches or leaks occur.

Third Party: The data user must use contractual or other means to:

- Prevent unauthorized or accidental access, processing, erasure, or loss of use of the personal data; and
- Ensure that the data processor does not retain the personal data for longer than necessary.

Breach Notification

Not required by the Ordinance.

Enforcement

Failure to abide by an enforcement notice is a criminal offense, punishable by a fine of up to HK\$50,000 and imprisonment for up to two years, as well as a daily penalty of HKD\$1,000 if the offense continues after conviction.

XXIX. Hungary

See GDPR discussion.

XXX. India

Information Technology Rules, No. 21 of 2000, Acts of Parliament, 2011 (India)

India's IT Ministry adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules ("Privacy Rules") in 2011.

Personal Information

Personal information is defined as any information that relates to a natural person, which either directly or indirectly, in combination with other information that is available or likely to be available to a corporate entity, is capable of identifying such person. Sensitive personal information includes:

- Passwords;
- Financial information;
- Physical, physiological and mental health condition;
- Sexual orientation;
- Medical records and history; and
- Biometric information.

Data Protection Officer

A company must appoint a Grievance Officer to address complaints related to the processing of personal information, and to respond to individual's requests for access or correction.

Collection & Processing of Personal Information

A company that collects, receives, possesses, stores, deals or handles information, shall provide a privacy policy that discloses the practices regarding the handling and disclosure of personal information including sensitive personal information. The following must be provided:

- The fact that the information is being collected;
- The purpose for which the information is being collected;
- The intended recipients of the information; and
- The intended recipients of the information.

To collect sensitive information, a company must receive **express** consent. Sensitive information may only be collected for a lawful purpose connected with a function or purpose of the corporate entity, and only if such collection is considered necessary for that purpose.

Transfer of Personal Information

A company must obtain the consent of the provider of information for any transfer of **sensitive personal information** to any other corporate entity or person in India, as well as any other country with data security as provided for under the Privacy Rules.

Security of Personal Information

A company must implement and maintain reasonable security practices and procedures to secure the personal information.

Breach Notification

The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (Cert-In Rules) impose mandatory notification requirements on a company upon the occurrence of certain cyber security incidents.

Cyber security incidents have been defined to mean any real or suspected adverse events, in relation to cyber security, that violate any explicitly or implicitly applicable security policy, resulting in:

- Unauthorized access, denial or disruption of service;
- Unauthorized use of a computer resource for processing or storage of information;
- Changes to data, information without authorization.

The occurrence of the following types of cyber security incidents, trigger the notification requirements under the rules:

- Targeted scanning/probing of critical networks/systems;
- Compromise of critical information/system;
- Unauthorized access of IT system/data;
- Defacement of websites or intrusion into website & unauthorized changes such as inserting malicious codes, links to external websites;
- Malicious code attacks such as spreading virus, worm/Trojan/Botnets/Spyware;
- Attacks on servers such as Database, Mail and DNS & Network devices such as Routers;
- Identity theft, spoofing and phishing attacks;
- Denial of service & Distributed Denial of service attacks;
- Attacks of critical infrastructure, SCADA systems and wireless networks;
- Attacks on application such as E-governance and E-commerce.

Upon occurrence of any of the aforementioned events, a company is required to notify the Cert-In within reasonable time, as to leave scope for appropriate action by the authorities.

Enforcement

Civil penalties of up to EUR 694,450 for failure to protect personal information including sensitive personal information may be imposed; damages in a civil suit may exceed this amount. Also, criminal penalties of up to three years or a fine of EUR 6,950, or both for unlawful disclosure of information.

XXXI. Ireland

See GDPR discussion.

XXXII. Israel

Human Dignity and Liberty, 5752 – 1992 (Isr.)

Protection of Privacy Law, 5741 – 1981 (Isr.)

The collection and processing of personal information in Israel is governed by the Basic Law: Human Dignity and Liberty, 5752 – 1992; the Protection of Privacy Law, 5741 – 1981 and the regulations promulgated thereunder (the “PPL”).

Personal Information

Personal information is defined as data regarding the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person. Sensitive personal information means data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person.

Registration

Subject to limited exceptions, a database registration is required to the extent one of the following conditions are met:

- The database contains information in respect of more than 10,000 individuals;
- The database contains sensitive information;
- The database includes information on persons, and the information was not provided by them, on their behalf or with their consent;
- The database belongs to a public entity; or
- The data base is used for direct-marketing services.

Data Protection Officers

A company must appoint a data protection officer if a company meets one of the following conditions:

- A possessor of five databases that require registration;
- A public body; or
- A bank, an insurance company or a company engaging in rating or evaluating credit.

Collection and Processing of Personal Information

The collection, processing or use of personal information is permitted subject to obtaining the informed consent of the individual. Consent should be obtained for specific purposes of use, the processing and use of personal information should be proportionate to those purposes, and data subjects should have the right to inspect and correct their personal information.

A request for consent must be accompanied by a notice indicating the following:

- Whether there is a legal requirement to provide the information;
- The purpose for which the information is requested;
- The recipients of the personal information, and
- The purpose(s) of use.

Transfer of Personal Information

The Privacy Protection Regulations govern the transfer of personal information abroad. Personal information may only be transferred abroad to the extent that:

- The laws of the country ensure a level of protection no lesser than that provided by Israeli law; or
- One of the following conditions are met:
 - The individual has consented;
 - The consent cannot be obtained and the transfer is vital to the protection of his or her health or physical wellbeing;
 - The information is transferred to a corporation under the control of the owner of the database from which the data is transferred, provided that such corporation has guaranteed the protection of privacy after the transfer;
 - The data is transferred to an entity bound by an agreement with the database owner, to comply with the conditions governing the use of the data as applicable under Israeli Laws;
 - Data was made public;

- Transfer of data is vital to public safety or security;
- Transfer is required by law;
- Transferred to specific countries under the regulations.

When transferring personal data abroad, the database owner is required to enter into a data transfer agreement with the data recipient, pursuant to which the recipient undertakes to apply adequate measures to ensure the privacy of the data subjects and guarantees that the data shall not be further transferred to any third party.

Security of Personal Information

On March 21, 2017, the Constitution, Law, and Justice Committee of the Knesset approved the Data Security Regulations (“DSRs”). The DSRs impose additional security requirements, including: having in place a broad list of manuals and policies; various physical, environmental and logical security measures; and regular audit, inspection and training obligations.

Breach Notification

According to the DSRs, data breach notifications are required depending on the severity of the breach and the category of the database. Such notifications are generally to the Israel Privacy Authority which may require further notification to the data subjects.

Enforcement

Breach of the PPL may result in both civil and criminal sanctions, including administrative fines, 1-5 years of imprisonment, and the right to receive statutory damages under civil proceedings without the need to prove actual damages.

XXXIII. Italy

See GDPR discussion.

XXXIV. Japan

Act on the Protection of Personal Information, No.57 of 2003 (Japan)

The Japan Act on the Protection of Personal Information (“APPI”) was amended and came into effect on May 30, 2017. The Personal Information Protection Commission (“PPC”) acts as a supervisory governmental organization on issues of privacy protection.

Personal Information

Personal information means that information relating to a living individual can identify a specific individual by name, date of birth, or other description contained in such information. Personal

information includes information which enables one to identify a specific individual with easy reference to other information.

Personal information also includes any “Personal Identifier Code.” This refers to certain types of data specified under a relevant cabinet order of the APPI, and includes biometric data which can identify a specific individual, or data in the form of a certain code uniquely assigned to an individual.

Sensitive information includes information about a person’s race, creed, social status, medical history, criminal record, any crimes a person has been convicted of, and any other information that might cause the person to be discriminated against.

Anonymized information refers to any information about individuals from which all personal information has been removed and such removed personal information cannot be restored. If a business operator has sufficiently anonymized the information, it can be used beyond the purpose of use notified to the individual and disclosed to third-parties without requiring the consent of the individual.

Data Protection Officer

Not required by the APPI.

Collection & Processing of Personal Information

A company must specify the purpose for which the information is collected and processed. Once collected, a company may not use the information for an additional purpose, nor should it use the information outside the scope of that is necessary for the achievement of that purpose.

The purpose must be made known to the individuals when personal information is collected or promptly thereafter and this can be made by public announcement. When information is obtained by way of contract or other document, the company must expressly state the purpose of the collection. This must be done in a reasonable manner.

The guidelines to the APPI suggest the appropriate method for a website to announce the purpose is a one click access on the homepage so that the individual can easily find the purpose of use before submitting the personal information.

Transfer of Personal Information

Personal information may not be disclosed to a third party without the prior consent of the individual, unless the company handling the personal information adopts the opt-out method and provides an advance notice of joint use.

Additionally, the disclosure of personal information between group companies is considered disclosing the information to a third-party, and thus consent must be obtained unless it meets the requirements of joint use. The APPI also has permitted the opt out method, whereby a business can as a default disclose personal information to third parties, unless individuals opt out of allowing

the business operator to do so. The APPI requires a business to preemptively disclose to the PPC, and the public or to the individual of the following:

- The purpose of use includes the provisions of such information to third parties and the method of such provision;
- The nature of the personal data provided to third parties;
- The method by which personal data is provided to third parties;
- The matter that provision of such information to third parties will be stopped upon the request of the individual;
- The method for an individual to submit an opt out request to the company.

Security of Personal Information

The APPI requires that a company prevent the leakage of personal information. However, the APPI does not set forth specific steps to ensure protection; rather, the guidelines indicate that necessary and appropriate measures generally include “Systematic Security Control Measures,” “Human Security Control Measures,” “Physical Security Measures” and “Technical Security Control Measures.”

Breach Notification

It is not legally required to report a data breach under the APPI.

Enforcement

A company may be requested to submit a report, the PPC may conduct on-site inspection and request or order the business operator handling personal information to take remedial actions. If a business operator handling personal information does not submit the report or materials, or reports false information they will be subject to a fine of up to JPY 300,000. If a company does not follow an order from the PPC they will be subject to a penalty of up to six months or a fine of up to JPY 300,000.

An unauthorized disclosure of personal information, for the benefit of the disclosing party or any third party, will be subject to a penalty of imprisonment for up to one year or a fine of up to JPY 500,000.

Adequacy Decision by EU

On January 23, 2019, the European Commission adopted an adequacy decision on the protection of personal information in Japan. See http://europa.eu/rapid/press-release_IP-19-421_en.htm. The European Commission has found that Japan's data protection legislation and practice constitutes an "adequate framework" based on an analysis of the Japanese Act on the Protection of Personal Information ("APPI") already in place, together with the newly agreed Supplementary Rules (the "Rules"). As of the adequacy decision date, the Rules are in force and

legally binding on Japanese Business Operators handling EU personal data and are enforceable by Japan's Personal Information Protection Commission ("PPC"). In parallel, Japan adopted its equivalent decision.

In practice, with the adoption of the adequacy decisions, EU and Japanese businesses are now able to transfer data between them without being required to provide further safeguards or being subject to additional conditions. This means that the requirements of Article 46 of the GDPR imposing appropriate safeguards for international data transfer ceases to apply to data transfer between the EU and Japanese companies. The reciprocal adequacy decisions therefore allow companies to freely exchange personal data of their employees and customers without having to engage in burdensome paperwork.

The European Commission also drafted a “fact sheet” to highlight certain “guarantees” provided by the newly impended Rules which also apply under the GDPR. Japanese Business Operators must be mindful of the following requirements when handling EU personal data:

- Data is only processed for the purpose for which they were legally transferred from the EU, unless EU citizens give their consent for processing for a different purpose;
- Data is processed to the extent necessary for this purpose;
- Data is kept no longer than necessary for this purpose;
- Data is kept accurate and up to date;
- Data is never further transferred to individuals or entities abroad which do not guarantee an adequate level of protection, unless consent of EU individuals is obtained for such transfer;
- The processing should be done under appropriate security measures, protected against unauthorized or unlawful processing and against accidental loss, destruction or damage;
- Additional safeguards apply to sensitive data (data revealing health conditions, sexual orientation, political opinions, etc).

See

https://ec.europa.eu/info/sites/info/files/research_and_innovation/law_and_regulations/documents/adequacy-japan-factsheet_en.pdf.

XXXV.Latvia

See GDPR discussion.

XXXVI. Lithuania

See GDPR discussion.

XXXVII. Luxembourg

See GDPR discussion.

XXXVIII. Malaysia

Personal Data Protection Act, No. 709 (2010)

The Personal Data Protection Act of 2010 (“PDPA”) came into force on November 3, 2013.

Personal Information

Personal information means any information in respect of commercial transactions, which

- Is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
- Is recorded with the intention that it should wholly or partly be processed by means of such equipment; or
- Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

That 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.

Sensitive personal information means any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offense or any other personal data as the Minister of Communications and Multimedia may determine by order published in the Gazette.

Registration

The PDPA recognizes classes of data users who must be registered. The classes which have been identified are: Communications, Banking and Financial Institutions, Insurance, Health, Tourism & Hospitalities, Transportation, Education, Direct Selling, Services, Real Estate, and Utilities. There are fees chargeable for registration and the registration is valid for 24 months, after which renewal is required.

Principles

The PDPA asserts seven principles which have to be complied with when processing personal information. Non-compliance by a company with any of the principles constitutes an offense under the PDPA and the penalty includes fines and/or imprisonment

General Principle

This principle prohibits a company from processing an individual’s personal information without their consent. Consent must be “recorded” and “maintained.” Consent is not required:

- For the performance of a contract to which the data subject is a party;
- For the taking of steps at the request of the data subject to entering into a contract;
- For compliance with a legal obligation;
- To protect the vital interests of the data subject;
- For the administration of justice; or
- For the exercise of any functions conferred on any person by or under any law.

Explicit consent is required for the processing of sensitive personal information.

The PDPA also prohibits processing of personal information unless it is for a lawful purpose directly related to the activity of the data user.

Notice and Choice Principle

A company shall by written notice inform a data subject:

- Describe the personal information being processed;
- The purpose for which it is being collected or processed;
- Any information as to the source of the personal information;
- Right to request access or correction, and how to contact the company with inquiries or complaints;
- The class of third parties to whom the information may be disclosed;
- Choices and means the company offers the individual for limiting the processing of personal information;
- Whether it is obligatory or voluntary to supply the personal information; and
- The consequences if he/she fails to supply the information.

The information shall be given as soon as practicable.

Disclosure Principle

No personal information shall, without the consent of the individual, be disclosed for any purpose other than:

- The purpose for which it was collected; or

- A purpose directly related to the original purpose.

Security Principle

A data user shall take practical steps to protect personal information from loss, misuse, modification, unauthorized or accident access or disclosure, and alteration or destruction.

Retention Principle

The personal data processed for any purpose shall not be kept longer than is necessary for the fulfillment of that purpose. A company shall take reasonable steps to ensure that all personal information is destroyed or permanently deleted it is no longer required for that purpose.

Data Integrity Principle

A company shall take reasonable steps to ensure accurate, complete, and not misleading personal information.

Access Principle

The data subject shall be given access to the personal information.

Transfer of Personal Information

Under the PDPA, a company may not transfer personal information to a jurisdiction outside of Malaysia unless that jurisdiction has been specified by the Minister. However, certain exceptions apply, such as:

- The data subject has given consent;
- The transfer is necessary for the performance of a contract between the data subject and data user;
- The data user has taken all reasonable steps and exercised all due diligence to ensure that the personal data will not be processed in a manner which, if that place were Malaysia, would contravene the PDPA; and
- The transfer is necessary to protect the data subject's vital interests.

Breach Notification

There is no requirement under the PDPA for data users to notify authorities regarding data protection breaches in Malaysia.

Enforcement

Violations of the PDPA and certain provisions of the Personal Data Protection Regulations attracts criminal liability. The prescribed penalties include the imposition of fines or a term of

imprisonment, or both. Directors, CEOs, managers or other similar officers will have joint and several liability for non-compliance by the body corporate, subject to a due diligence defense.

XXXIX. Mexico

Federal Law on Protection of Personal Data Held by Private Parties, art. 1-33 Gaceta Oficial [GO] (Mex.)

The Federal Law on Protection of Personal Data Held by Private Parties (“Privacy Law”) was enacted on July 5, 2010 and entered into force on July 6, 2010.

Definitions - What is Regulated

For the purpose of this law, the following definitions apply:

- Personal Data: “Any information concerning an identified or identifiable individual.”
- Sensitive Personal Data: “Items such as racial or ethnic origin, present and future health status, genetic information, religion, philosophical and moral beliefs, union membership, political views, sexual preference.

The processing of personal information includes the retrieval, use, disclosure, or storage of personal data by any means. The use of personal data includes any action related to its access, management, commercial use, transfer, or disposal.

Principles of Personal Data Protection

Data controllers must adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality, and accountability under the Law. Personal data must be collected in a **lawful** manner.

In all processing of personal data, it is presumed that there is a **reasonable expectation of privacy**.

Consent

All processing of personal data will be subject to the **consent** of the data owner, which may be verbal, in writing, electronic or optical means or by unmistakable indications. Consent may be revoked at any time. In the case of sensitive personal data, the data controller must obtain **express written consent** from the data owner through signature, electronic signature, or any authentication mechanism established for such a purpose.

The data controller **shall** ensure the personal data is **relevant, correct, and up-to-date** for the purposes for which it has been collected. When the personal data **is no longer** necessary, it must be cancelled.

Privacy Notice

The data controller must provide a **privacy notice** to the data owner, which is defined as a document that is made available to the data owner prior to the processing of his personal information. The privacy notice must contain at least the following information:

- The identity and domicile of the data controller collecting the data;
- The purpose of the data processing;
- The option and means offered to limit the use or disclosure of data;
- The means for exercising rights of access, rectification, cancellation or objection;
- Where appropriate, the data transfers to be made;
- The procedures and means by which the data controller will notify the data owners of changes to the privacy notice;
- For sensitive personal data, the privacy notice must expressly state that it is dealing with his type of data.

The privacy notice must be made available to data owners through print, digital, visual or audio formats or any other technology as follows:

- **Personally:** the privacy notice must be provided at the time the data is collected, clearly and unequivocally, through the format by which collection is carried out, unless provided prior.
- **Electronic, Optical, Audio, or Visual Means:** the data controller must provide the its identity and domicile, the purpose of the data processing, as well as the mechanisms for the data owner to obtain the full text of the privacy notice.

Security Measures

All responsible parties that process personal data **must** establish and maintain physical and technical administrative **security measures** designed to protect personal information from damage, loss, alteration, destruction or unauthorized use, access or processing.

Security breaches occurring at any stage of processing that **materially affect** the property or moral rights of data owners will be reported immediately by the data controller to the data owner, so that the latter can take appropriate action to defend its rights.

Rights of Data Owners

Data owners will have the right to **access** their personal information, **rectify** data if it is inaccurate or incomplete, and the right to **cancel** his personal data. The data controller will not be obligated to cancel under the certain circumstances.

Data owners, will at all times and for any legitimate reason, have the right to **object** to the processing of their data.

Exercise of Rights of Access, Rectification, Cancellation and Objection

The data owner may at any time make a request for **access, rectification, cancelation, or objection** in relation to the personal data concerning him.

The data controllers must designate an individual or department who will process these requests. The data controller must notify the data owner within a maximum of **twenty days** of the request for access, rectification, cancelation or objection of the determination made.

Refusal may be made in the following cases:

- Where the requesting party is not the subject or legal representative of the data;
- The personal data is not found;
- The rights of a third party are adversely affected;
- Where there is a legal impediment;
- If the request has been previously performed.

Data Transfer

Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it must provide them with the privacy notice and the purposes to which the data owner has limited data processing.

Domestic or international transfers of data may be carried out without the consent of the data owner in the following cases:

- Where the transfer is necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management;
- Where the transfer is made to a holding company, subsidiary or affiliate under common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies;
- Where the transfer is necessary by virtue of a contract executed or to be executed in the interest of the data owner between the data controller and a third party;
- Where the transfer is necessary or legally required to safeguard public interest;

Penalties

Violation of the law may result in monetary penalties or imprisonment:

- A monetary sanction may be imposed from 100 to 320,000 times the Mexico City minimum wage. With regard to violations committed concerning the processing of sensitive personal data, sanctions may be increased up to double the above amounts.
- Three months to three years may be imposed on any person authorized to process personal data who, for profit, causes a security breach affecting the databases under its custody. Penalties will be doubled if the sensitive personal data is involved.
- Six months to five years imprisonment may be imposed on any person who, with the aim of obtaining unlawful profit, processes personal data deceitfully, taking advantage of an error of the data subject or a person authorized to process such data. Penalties will be doubled if sensitive personal data is involved.

XL. Monaco

Data Protection Law, No. 1.165 of 23 (1993), No. 1.353 (2008), No.1.454 (2018)

Personal information is protected in Monaco by the Data Protection Law (“DPL”) which was last modified on October 30, 2018.

Personal Information

Personal information is defined as “data enabling identification of a determined or indeterminable person. Any individual who can be identified, directly or indirectly, notably by reference to an identification number or to one or more factors specifically to his physical psychological, economical, cultural, or social identity is deemed to be identifiable.”

Sensitive personal information is “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health/genetic data, sex life, data concerning morals or social matters.”

Registration of Personal Information

A company must inform/notify/request approval from the Commission for Control of Personal Data (“CCPD”) so that their processing may be registered. Any changes will require the registration to be amended.

The notification shall include:

- What data is being collected;
- Why the data will be processed;
- The categories of the data subject; and
- Whether the data will be transferred within or outside of Monaco.

Data Protection Officer

Not required by the DPL.

Collection and Processing of Personal Information

According to the DPL, the processing of personal information must be justified by:

- The individual's consent;
- A legal duty imposed on the company;
- A public purpose;
- Contract between the company and the individual; or
- The company's legitimate interest, subject to the individual's rights and liberties.

The company must provide the individual with fair processing information. This includes the identity of the company, the purpose of the processing, and any other information needed under the circumstances to ensure that the processing is fair.

Transfer of Personal Information

The DPL requires the transfer of personal information only to a country with equivalent protection and reciprocity. The CCPD established a list of acceptable countries.

Security of Personal Information

A company must take appropriate technical and organizational measures against unauthorized or unlawful processing and against accidental loss or destruction of, or damage to, personal data.

Breach Notification

Not required by the DPL.

Enforcement

Failure to comply with an enforcement notice is a criminal offence punishable of 1 month to 1 year of imprisonment or a fine of between EUR \$9,000 -- \$90,000 or both.

XLI. Netherlands

See GDPR discussion.

XLII. New Zealand

Privacy Act of 1993, No. 28 (N.Z.)

The collection, use, disclosure, storage, and retention of personal information is governed by the Privacy Act of 1993 (“Act”).

Personal Information

Personal information is defined as information about an identifiable individual, and includes information relating to a death. There is no differentiation between personal information and sensitive personal information.

Data Protection Officer

The Act requires a company to appoint one or more individuals to be a privacy officer. The responsibilities for the privacy officer include:

- The encouragement of compliance, by the company, with the information privacy principles;
- Dealing with requests made to the company pursuant to the Act;
- Working with the Privacy Commissioner (responsible for enforcing the Act) in relation to investigations conducted in relation to the company;
- Otherwise ensuring compliance with the company with the provisions of the Act.

Collection and Processing of Personal Information

A company may collect, store, and process personal information in accordance with the following twelve information privacy principles:

- The personal information is needed for a lawful purpose connected with the company’s work;
- The personal information is collected directly from the relevant person;
- Before the personal information is collected, the agency has taken reasonable steps to ensure that the person knows that the information is being collected; the purpose for which it is being collected; the intended recipients; the name and address of the agency collecting and holding the information; if the information is authorized or required by law, the applicable law and the consequences if the requested information is provided; and that the person concerned may access and correct the information;
- The personal information is not collected in an unlawful or unfair way or in a way that unreasonably invades a person’s privacy;
- The personal information must be kept reasonably safe from being lost, accessed, used, modified or disclosed to unauthorized persons;

- The personal information is readily retrievable, the relevant person is entitled to know whether information is held and to have access to it;
- The relevant person is entitled to request correction of the personal information. If the agency will not correct the information, the person may provide a statement of the correction sought to be attached to the personal information;
- Before it is used, the company must ensure that the personal information is accurate, up to date, complete, relevant, and not misleading;
- The personal information may not be kept for any longer than it is needed;
- Subject to certain exceptions, personal information collected for one purpose may not be used for another purpose;
- A company must not disclose personal information to another person, body or company except in specific circumstances;
- A company may only assign a unique identifier to an individual if it is needed for the company to carry on its work efficiently and may not assign a unique identifier to an individual if the same identifier is used by another agency.

Personal information does not need to be collected directly from the relevant person if:

- The personal information is publicly available;
- The relevant person authorizes collection of the personal information from someone else;
- Non-compliance would not prejudice the interests of the relevant individual;
- The personal information is being collected for a criminal investigation, enforcement of a financial penalty, protection of public revenue or the conduct of court proceedings;
- Compliance would prejudice the purpose of the collection of the personal information or is not practical in the circumstances; and
- The personal information will be used in a way which will not identify the person concerned.

Transfer of Personal Information

A company should not disclose personal information to another entity unless the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained. Care must be taken that all safety and security precautions are met to ensure the safeguarding of that personal information to make certain that it is not misused or disclosed to any other party.

The Privacy Commissioner is given the power to prohibit a transfer of personal information from New Zealand to another state, territory, province or other part of a country by issuing a transfer prohibition notice.

Security of Personal Information

A company shall ensure that personal information is kept securely and protected by such security safeguards as are reasonable in the circumstances to protect against:

- Loss;
- Access, use, modification or disclosure, except with the authority of the agency; and
- Other misuse or unauthorized disclosure.

If disclosed to a third-party, the company must do everything reasonably within its power to prevent unauthorized use or unauthorized disclosure of the information.

Breach Notification

Not required by the Act.

Enforcement

The Privacy Commissioner may initiate a formal investigation and issue an opinion on how the Act applies to a complaint. The Privacy Commissioner may refer the matter to the Director of Human Rights who may decide to take a complaint to the Human Rights Review Tribunal. The Tribunal may award damages against the defendant for an interference with the privacy of an individual in a one or more of the following:

- Pecuniary loss suffered as a result of, and expenses reasonably incurred by the aggrieved individual for the purpose of, the transaction or activity out of which the interference arose;
- Loss of a benefit, whether or not of a monetary kind, which the aggrieved individual might reasonably have been expected to obtain but for the interference;
- Humiliation, loss of dignity, and injury to the feelings of the aggrieved individual.

XLIII. Norway

See GDPR discussion.

XLIV. Poland

See GDPR discussion.

XLV. Portugal

See GDPR discussion.

XLVI. Qatar

Personal Data Protection, Law No. 13 of 2016 (Qatar)

The Law No. (13) of 2016 Concerning Personal Data Protection (“CPDP”) was passed on November 3, 2016.

Personal Information

Personal information is defined as data belonging to an individual with specified or reasonably specifiable identity whether through such Personal Data or through combining the same with any other data. Sensitive personal information relates to the racial origin, children, health condition, physical condition, psychological condition, religious beliefs, spousal relation, and/or criminal crimes.

Data Protection Officers

Not required by the CPDP.

Collection and Processing

Unless proscribed by law, a company may only process personal data **after** obtaining the individual’s consent.

Prior to processing, the company shall notify the individual of:

- The details of the company or another party who processes the data on behalf of the company;
- The purpose for which the company desires to process the personal information;
- Full and precise description of the processing activities and the levels of disclosure of such personal information;
- Any other information necessary and required to meet the requirements of processing personal information.

A company shall also follow the following obligations:

- Process the personal information honestly integrally and legitimately;
- Process the controls on designing, changing and/or developing personal information – related products, systems and services; and

- Take appropriate administrative, technical and physical precautions as necessary to protect personal information; and
- Abide by the privacy protection policies developed by the Competent Department and decreed by the Minister.

Consent is **not required** under the following circumstances:

- Executing a public interest-based task as per applicable laws; and/or
- Enforcing a legal obligation or a competent court order; and/or
- Protecting vital interests of an individual; and/or
- Achieving public interest-based scientific research purposes; and /or
- Collecting personal information needed for a criminal crime investigation.

Sensitive personal information may not be processed except after obtaining authorization from the Qatar Ministry of Transport and Communications (MoTC).

Transfer of Personal Information

The Controller shall not take any decision or adopt a measure that may limit the cross-boundary personal data flow unless the underlying processing falls foul of the CDPD or may cause serious damage to the personal information or to the individual's privacy.

Security of Personal Information

A company must take appropriate technical and organizational measures to securely manage personal information. The company must carry out the following procedures:

- Review privacy protection measures before proceeding with new processes; and
- Determine the processors responsible for protection of personal information; and
- Train, and raise the awareness of, the processors in the protection of personal information; and
- Develop an internal system to receive and look into complaints, data access requests and omission/correction request; and shall provide access thereto to individuals; and
- Develop an internal effective personal data management system, and report any breach of protection measures thereof; and
- Use appropriate technologies to enable individuals to exercise their rights to directly access, review and correct their respective Personal Data; and

- Conduct comprehensive audits and reviews on the compliance with personal data protection requirements; and
- Ensure processors' compliance with the instructions given thereto, adoption of appropriate precautions to protect personal data, and follow through on the same constantly.

Breach Notification

There is an obligation on a company to notify the regulator, the MoTC and the individual of any breaches of the measures to protect the individual's privacy if it is likely to cause damage to the individual.

Enforcement

The MoTC can impose fines of up to QAR 5,000,000 for violations of the CDPD.

XLVII. Romania

See GDPR discussion.

XLVIII. Russia

Data Protection Act, No. 152 FZ (2006)

The rules regarding the collection and processing of personal information are found in the Data Protection Act No. 152 FZ dated July 26, 2006 ("DPA").

Personal Information

Personal information is defined as any information that relates directly or indirectly to the specific or defined physical person. Sensitive personal information is defined as special categories of persona data in Russian legislation. Such special categories include data related to race, national identity, political opinions, religious and philosophical beliefs, health state, intimacies and biometrical data.

Registration of Personal Information

The Federal Service for Supervision of Communications, Information Technologies and Mass Media is responsible for maintaining the Registry of Data Controllers ("Agency"). Any company shall notify the Agency in writing about its intention to process personal information, unless one of the following exclusions applies:

- The personal data is exclusively data about employees;
- The personal data was received in connection with a contract entered into with the individual, provided that such data is not transferred without the consent of the

individual, but used only for the performance of the contract and entering into contracts with the individual;

- The personal information is the data about members of a public or religious association and processed by such an organization for lawful purposes in accordance with their charter documents, provided that such data is not transferred without the consent of the individuals;
- The personal information was made publicly accessible by the data subject;
- The personal information includes the surname, name and father's name only;
- The personal information is necessary in order to give single access to the premises of the company or for other similar purposes;
- The personal information is included in state automated information systems or state information systems created for the protection of state security and public order;
- The personal information is processed in accordance with the law without any use of automatic devices; or
- The personal data is processed in accordance with transportation security legislation for the purposes of procurement of stable and secure transport complex and personal, community and state interest protection.

The notification letter shall contain information about:

- The full name and address of the data controller;
- The purpose of the processing;
- The categories of personal data processed;
- The categories of the subjects whose personal data is processed;
- The legal grounds for processing;
- The types of processing of the personal data;
- Name and contact information of the physical person or legal entity responsible for personal information processing;
- The commencement date;
- Information on occurrence of cross border transfer of personal information;

- The term of processing or the conditions for termination of processing the personal information;
- Information on personal information security provision.

Data Protection Officers

A company is required to appoint a data protection officer. Non-appointment or improper appointment of the data protection officer is a violation of the data protection regime and may result in the imposition of penalties and enforcement protocols, as described below.

Collection and Processing of Personal Information

A company may collect and process personal information where the following conditions are met:

- The individual consents;
- The processing is required by a federal law or international treaty;
- The processing is required for administration of justice, execution of a court order or any other statements of public officers to be executed;
- The processing is required for provision of state or municipal services;
- The data controller needs to process the data to perform or conclude a contract to which the data subject is a party or beneficiary party or guarantor;
- The processing is carried out for statistical or scientific purposes provided that it is impersonalized;
- The processing protects the company's interests and it is impossible to have the individual's consent;
- The processing is required for execution of statutory controller's or third parties' rights or for purposes important for the community provided the data subject's rights are not in breach;
- Personal information that is processed was public;
- The processing is carried out by a journalist or mass media as part of its professional activities or for the purposes of scientific, literary or other creative activities, except if the processing would damage the data subject's rights and freedoms; or
- Personal information that is processed is subject to publication or mandatory disclosure under law.

In the following cases, the DPA requires that the individual's consent should be in writing:

- Where the personal information collected to be included within publicly accessible sources;
- Where sensitive or biometric data is processed;
- In the case of the cross boarder transfer of personal data, where the recipient state does not provide adequate protection of personal information; or
- Where a legally binding decision is made solely on the grounds of the automated processing of personal data.

Consent in writing must contain the following:

- The identity of the individual, his/her address and passport details;
- Data representative (if any);
- The identity and address of the company or the entity that processes personal information of the company (if any);
- The purpose of the processing;
- The list of personal information that may be collected and processed;
- The types of processing that are authorized;
- The term for which the consent, remains valid and way of revocation; and
- The individual's signature.

Transfer of Personal Information

A company must ensure that the recipient of personal information provides adequate protection of personal information **before** transferring. Where there is no adequate protection of personal information, a cross border transfer is permitted if one of the following conditions is met:

- The individual consents;
- The transfer is provided for under an international treaty to which Russia is a signatory;
- The transfer is necessary in accordance with federal laws for protection of the Constitution, state defense, security, and transport system;
- For the purposes of performance of a contract to which the data subject is a party; or
- The transfer protects the data subject's vital interests where it is not possible to get the written consent of the data subject.

Security of Personal Information

A company is required to take appropriate technical and organizational measures against unauthorized or unlawful processing and accidental loss, changing, blocking or destruction of, or damage to, personal information.

Breach Notification

Not required by the DPA.

Enforcement

The maximum administrative penalty that can be imposed is RUR 75,000.

XLIX. Singapore

Personal Data Protection Act, No. 26 of 2012 (SG)

The rules regarding the collection and processing of personal information are found in the Personal Data Protection Act of 2012 (“Act”). The Act has extraterritorial effect, and so applies to organizations collecting personal data from individuals in Singapore whether or not the organization itself has a presence in Singapore.

Personal Information

Personal information is defined to mean, whether true or not, about an individual, whether living or recently deceased (ten years or fewer), who can be identified:

- From that data; or
- From that data and other information to which the organization has or is likely to have access.

The Act does not define sensitive personal information.

Data Protection Officers

A company must appoint one or more data protection officers (“DPO”) to be responsible for ensuring compliance with the Act. The contact information of the DPO must be made available to the public.

Failure to appoint a DPO may lead to a preliminary investigation by the Personal Data Protection Commission. Failure to cooperate with the Commission will constitute an offense, which may result in a fine of up to \$10,000 or imprisonment for a term not exceeding 12 months, or both. A company may be subject to a fine of \$100,000.

Collection and Processing of Personal Information

A company may collect, use, or disclose personal information if:

- They obtain express consent from the individual prior to the collection, use, or disclosure of the personal information, and have also provided the relevant data protection notice to the individual on or before collecting, using or disclosing personal data; or
- There is deemed consent by the individual to the collection, use, or disclosure of personal information with the relevant conditions of the Act; or
- If no consent or deemed consent is given, if limited specific exclusions prescribed in the Act apply.

Collection, use, or disclosure of personal information must only be for the purposes that a reasonable person would consider appropriate in the circumstances, and for purposes to which the individual has been notified of.

A company may collect, use, or disclose personal information **without consent** if (irrelevant examples omitted):

- The collection is necessary for any purpose that is clearly in the interest of the individual, if consent for its collection cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;
- Necessary to respond to an emergency that threatens the life, health, or safety of the individual;
- Publicly available information.

A company must also:

- Make information about its data protection policies, practices and complains process publicly available;
- Cease to retain personal information where it is no longer necessary for any business or legal purpose; and
- Ensure personal information collected is accurate and complete if likely to be used to make a decision about the individual or disclosed.

Transfer of Personal Information

An organization should ensure that it has obtained the individual's deemed or express consent to a transfer of information (unless exceptions apply) and, if this was not done at the time the personal information was collected, additional consent will be required (unless exemptions apply).

The Act also contains offshore transfer restrictions, which require an organization to ensure "comparable protection" to the standards set out in the act when transferring personal information outside of Singapore.

Security of Personal Information

A company must make reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risk.

Breach Notification

The Act does not require breach notifications.

Enforcement

Enforcement of the Act is carried out by the Commission. The powers of the Commission include giving directions to:

- Stop collection, use or disclosure of personal information in contravention of the Act;
- Destroy personal information collected in contravention of the Act;
- Provide or refuse access to or correction of personal information; and/or
- Pay a financial penalty not exceeding \$1 million.

Any person who has suffered loss or damage directly as a result of a contravention of the Act is also entitled to pursue a private action in court. However, where the Commission has made a decision with regard to the said loss or damage, a right of private action will only lie after the decision has become final as a result of there being no further right of appeal. The court may grant the plaintiff all or any of the following:

- Relief by way of injunction or declaration;
- Damages; and/or
- Such other relief as the court thinks fit.

L. Slovenia

See GDPR discussion.

LI. South Africa

Protection of Personal Information Act 4 of 2013 (S. Afr.)

The Protection of Personal Information Act (“POPI”) governs the processing of personal information, and was signed into law on November 19, 2013.

Personal Information

Personal information is defined as information relating to an identifiable, living, natural person, and where applicable, an identifiable juristic person, including:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin; colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief; culture, language and birth of the person;
- Information relating to the education, medical, financial, criminal or employment history of the person;
- Any identifying number, symbol, e-mail address, telephone number, location information, online identifier or other particular assignment to the person;
- The biometric information of the person;
- The personal opinions, views or preferences of the person;
- Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- The views or opinions of another individual about the person; and
- The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

Sensitive personal information is information concerning religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information or criminal behavior (to the extent that such information relates to the alleged commission of an offense or any proceedings in respect of any offense allegedly committed, or the disposal of such proceedings).

Data Protection Officer

The POPI requires the registration with the Information Regulator of a data protection officer prior to taking up their duties. The duties and responsibilities of the data protection officer include encouraging and ensuring compliance, by the body, with POPI; dealing with any requests made to that body in terms of the POPI; and working with the Information Regulator in relation to investigations by the Information Regulator in relation to that body.

Collection and Processing of Personal Information

Processing of personal information is any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

- The collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- Dissemination by means of transmission, distribution or making available in any other form; or

- Merging, linking, as well as blocking, degradation, erasure or destruction of information.

The POPI prescribes eight conditions for the lawful processing (which includes collection) of personal information: accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation.

- Condition 1 – Accountability
 - A company must ensure that all conditions are complied with during processing;
- Condition 2 – Processing limitation
 - Personal information must be processed lawfully and in a reasonable manner;
 - Personal information may only be processed if it is adequate, relevant, and not excessive.
 - Personal information may only be processed if
 - The individual consents;
 - Processing is necessary for the conclusion or performance of a contract;
 - Processing complies with an obligation imposed by law;
 - Processing protects a legitimate interest of the individual;
 - Processing is necessary for the performance of a public law duty by a public body; or
 - Processing is necessary for pursuing the legitimate interests of the responsible party.
- Condition 3 – Purpose Specification
 - Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party;
 - Personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected;
 - A responsible party must destroy or delete a record of personal information as soon as reasonably practicable after the responsible party is no longer authorized to retain.
- Condition 4 – Further Processing Limitation

- Further processing of personal information must be in accordance or compatible with the purpose for which it was collected.
- Condition 5 – Information Quality
 - A responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.
- Condition 6 – Openness
 - A responsible party must maintain the documentation of all processing operations;
 - If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of:
 - The information being collected;
 - The name and address of the responsible party;
 - The purpose of the collection;
 - Whether supplying the information is voluntary or mandatory;
 - The consequences for failure to provide information;
 - Any law authorizing the processing;
 - If the information will be transferred;
 - Any further information as necessary.
- Condition 7 – Security Safeguards
 - *See Security of Personal Information and Breach Notification below.*
- Condition 8 – Data Subject Participation
 - An individual has the right to access and correct personal information.

Transfer of Personal Information

A company in South Africa may not transfer personal information to a third party in another country unless:

- The recipient is subject a law, binding corporate rules or a binding agreement which:
 - Uphold principles for reasonable processing of the information that are substantially similar to the conditions contained in POPPI; and

- Includes provisions that are substantially similar to those contained in POPI relating to the further transfer of personal information from the recipient to third parties who are in another country;
- The data subject consents to the transfer;
- The transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request; and
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party, or the transfer is for the benefit of the data subject and:
 - It is not reasonably practicable to obtain the consent of the data subject to that transfer; and
 - If it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

Security of Personal Information

A company must secure the integrity and confidentiality of personal information in its possession by taking appropriate, reasonable technical and organization measures to prevent:

- Loss of, damage to or unauthorized destruction of personal information; and
- Unlawful access to or procession of personal information.

To comply with this obligation, a company must take reasonable measures to:

- Identify all reasonably foreseeable internal and external risks to personal information under its control;
- Establish and maintain appropriate safeguards against the risks identified;
- Regularly verify that the safeguards are effectively implemented; and
- Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

Breach Notification

Where there are **reasonable grounds** to believe that personal information has been access or acquired, the responsible party must notify:

- The Regulator; and

- The individual, unless it is not ascertainable.

The notification must be made **as soon as reasonably possible** after the discovery. A company may only delay if a public body determines that notification will impede a criminal investigation.

The notification must be in writing in one of the following ways:

- Mailed;
- Email;
- Placed in a prominent position on the website of the company;
- Published in the news media; or
- As may be directed by the Regulator.

The notification must provide the following information:

- A description of the possible consequences of the security compromise;
- The measures being or intended to be taken;
- A recommendation with regard to the measures to be taken by the individual; and
- If known, the identity of the unauthorized person who accessed the information.

Enforcement

Any person may submit a complaint to the Information Regulator alleging non-compliance with POPI. A court hearing proceedings may award an amount that is just and equitable including:

- Payment of damages as compensation for patrimonial and non-patrimonial loss suffered by a data subject as a result of breach of the provisions of this Act;
- Aggravated damages, in a sum determined in the discretion of the court;
- Interest; and
- Costs of suit on such scale as may be determined by the court.

LII. South Korea

Personal Information Protection Act, 2011, art.1-75 (S. Kor.)

The South Korea Personal Information Protection Act (“PIPA”) was enacted and became effective as of September 30, 2011. The purpose of the act is to provide for the processing of the personal

information for the purpose of enhancing the right and interest of citizens, and further realizing the dignity and value of the individuals by protecting their privacy from the unauthorized collection, leak, abuse or misuse of personal information.

Personal Information

Personal information is information which contains information identifying a specific person with a name, a national identification number, images, or other similar information.

Sensitive personal information consists of information relating to an individual's:

- Thoughts or creed;
- History regarding membership in a political party or labor union;
- Political views;
- Health care and sexual life; and
- Other information stipulated under Presidential Decree

Data Protection Officers

Under PIPA, a company must designate a data protection officer. In the event a data protection officer is not assigned, the company may be subject to a maximum administrative fine of ten million.

Collection and Processing

As a general rule, a company may not handle personal information without obtaining prior consent, beyond the scope necessary for the achievement of the purpose of use.⁹⁸ If a company collects personal information, it must:

- First notify the data subject; and
- Obtain the data subject's prior consent to such collection.

If a company wishes to collect sensitive personal information, the consent must be separately obtained. Under the PIPA, a company must also notify the data subject of:

- The purpose of collection and use of the personal information;

⁹⁸ Relevant exceptions to the general rule above apply in the following cases under PIPA:

- where it is inevitable for a public institution to perform its affairs provided for in any Act and subordinate statute;
- where it is inevitably necessary for entering into and performing a contract with a subject of Personal Data;

- What is being collected;
- How long it will be possessed; and
- The individual's right to refuse to consent.

Transfer of Data

As a general rule, a company may not provide personal information to a third-party without prior opt in consent, with very limited exceptions. Under PIPA, a company must obtain consent after it notifies the subject of:

- The person to whom the data is furnished;
- The purpose of use;
- The types of personal information transferred;
- How long it will be possessed;
- The fact that the individual may refuse to consent and the consequences thereof.

Security

Under PIPA, a company must follow the following technical and administrative measures to prevent loss, theft, leakage, alteration, or destruction of personal information:

- Establish and implement an internal control plan for handling personal information;
- Installation of a control device to prevent access;
- Measures for preventing fabrication or alteration of records;
- Measures for security (including encryption);
- Measures for preventing intrusion of computer viruses;
- Any other measures necessary for securing the safety of personal information.

Breach

Under PIPA, the company must notify the individuals without delay of the details and circumstances, as well as remedial steps planned regarding a breach of personal information. If the number affects 10,000 individuals or more, the company shall notify the Ministry of the Interior, the Korea Internet & Security Agency, or the National Information Security Agency.

Enforcement

The Ministry of the Interior can take the following enforcement actions:

- Conduct investigations;
- Impose sanctions;
- Refer serious violations for criminal investigation.

The PIPA sets out detailed penalties for various types of violations, as follows:

- A data handler that commits a violation of the PIPA that constitutes a criminal offence may be subject to imprisonment of up to ten years or a fine of up to KRW100 million.
- For other violations, a data handler may be ordered to take corrective measures and/or be liable to an administrative fine of up to KRW50 million.
- In the case of loss, theft, leakage or falsification of resident registration numbers, a penalty surcharge of up to KRW500 million can be imposed on the data handler. To avoid this, the data handler must prove that it has taken all the necessary data security measures as prescribed by the PIPA.

Compensatory damages are available based on the PIPA. General tort principles as set out in the Civil Code may also apply, but the rules of the PIPA will prevail. Additionally, the PIPA provides for statutory and punitive damages.

A data subject whose personal data has been lost, stolen, or leaked due to a data breach can request damages of up to KRW3 million from the data handler if there has been any negligence or willful misconduct on the part of the data handler. The data handler can avoid liability by proving that it did not engage in willful misconduct or a negligent act. Data subjects are not required to prove the amount of damages they suffered.

Additionally, the court can order a data handler to compensate the aggrieved data subject up to three times the actual damages incurred if the data subject's personal data was lost, stolen, or leaked due to the data handler's gross negligence or willful misconduct.

LIII. Spain

See GDPR discussion.

LIV. Sweden

See GDPR discussion.

LV. Switzerland

Swiss Federal Act on Data Protection, (Bundesgesetz über den Datenschutz vom 19. Juni 1992), SR 235.1

The processing of personal information is regulated by the Federal Act on Data Protection (“DPA”) and its ordinances, *i.e.* the Ordinance to the Federal Act on Data Protection (“DPO”) and the Ordinance on Data Protection Certification (“ODPC”).

It should be noted that the DPA is subject to a substantial revision in an effort to comply with the GDPR.

Personal Information

Personal information means all information relating to an identified or identifiable natural or legal person. Sensitive personal information is defined as:

- Religious, ideological, political or trade union related views or activities;
- Health, the intimate sphere or racial origin;
- Social security measures; and
- Administrative or criminal proceedings and sanctions.

Registration

A company must register personal information files with the Federal Data Protection and Information Commissioner (“FDPIC”) before the files are opened, if:

- They regularly process sensitive personal data or personality profiles; or
- They regularly disclose personal information to third parties.

Data Protection Officers

There is no requirement under the DPA to appoint a data protection officer.

Collection and Processing of Personal Information

The following principles apply to the collection and processing of personal information:

- Personal information may only be processed lawfully, in good faith and according to the principle of proportionality;
- The collection of personal information and, in particular, the purpose of its processing must be evident to the data subject;
- Personal information should only be processed for a purpose that is indicated or agreed at the time of collection, evident from the circumstances at the time of collection, or provided for by law;
- The data controller and processor must ensure that the information is accurate;

- Personal information must not be transferred abroad if the privacy of the individual may be seriously endangered;
- Personal information must be protected from unauthorized processing by appropriate technical and organizational measures;
- Personal information must not be processed against the explicit will of the individual, unless justified by:
 - An overriding private or public interest; or
 - Law; and
- Sensitive personal information must not be disclosed to a third party, unless it is justified by:
 - The consent of the individual;
 - An overriding private or public interest; or
 - Law.

Transfer of Personal Information

Personal information may not be disclosed abroad if the privacy of the individual would be seriously endangered. In the absence of legislation that guarantees adequate protection, personal information may be disclosed abroad only if:

- Sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad;
- The data subject has consented in the specific case;
- The processing is directly connected with the conclusion or the performance of a contract and the personal information is that of a contractual party;
- Disclosure is essential in the specific case in order either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts;
- Disclosure is required in the specific case in order to protect the life or the physical integrity of the individual;
- The individual has made the information generally accessible and has not expressly prohibited its processing;
- Disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules that ensure an adequate level of protection.

The FDPIC maintains and publishes a list of such countries that offer an adequate level of protection.

Security of Personal Information

A company and any processor must take adequate technical and organization measures to protect personal information against unauthorized processing and ensure its confidentiality, availability and integrity. In particular, personal information must be protected against the following risks:

- Unauthorized or accidental destruction;
- Accidental loss;
- Technical errors;
- Forgery, theft or unlawful use; and
- Unauthorized altering, copying, accessing or other unauthorized processing.

The technical and organizational measures must be appropriate, in particular with regard to the purposes of the data processing, the scope and manner of the data processing, the risks for the data subjects and the current technological standards.

Breach Notification

There is no explicit statutory requirement to notify the FDPIC or the affected individuals under the DPA.

Enforcement

The DPA provides for criminal liability and fines of up to CHF 10,000 if a private person intentionally fails to comply with the following obligations under the DPA:

- Duty to provide information when collecting sensitive data and personality profiles;
- Duty to safeguard the data subject's right to information;
- Obligation to notify the FDPIC with regard to contractual clauses or binding corporate rules in connection with data transfers abroad;
- Obligation to register data files; or
- Duty to cooperate in an FDPIC investigation.

LVI. Taiwan

Personal Information Act, 2012, art. 1-56 Fawubu Quanguo Fagui Ziliaoku (ROC)

The processing of personal information is governed by the Personal Data Protection Law (“PDPL”), and was last amended and became effective on March 15, 2016.

Personal Information

Personal information means the name, date of birth, identification card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexual life, health checks, criminal records, contact information, financial conditions, social activities and other information which may directly or indirectly be used to identify a living natural person. Sensitive personal information means information relating to medical records, medical treatment, genetic information, sex life, health checks and criminal records.

Data Protection Officers

Not required under the PDPL.

Collection and Processing of Personal Information

Under the PDPL, a company should only collect personal information if there is a specific purpose and should comply with one of the following:

- Where collection or processing is explicitly stipulated by law;
- Where there is a contract or quasi contract between the company and individual and there is proper security measures in place;
- Where the individual had disclosed the information to the public;
- Where consent has been given by the individual;
- Where it is necessary to enhance the public interest;
- Where personal information is obtained from a publicly available source;
- Where there is no infringement on the rights of the individual.

A company must also unambiguously inform the individual of the following information prior or upon the collection of person information:

- The company’s name;
- Purposes for collection of personal information;
- Categories of personal information;
- Period, area, recipients and means of using the data;

- The data subject's rights and the methods by which the data subject may exercise those rights in accordance with the PDPL; and
- Where the data subject has the right to choose or not to provide the data and consequences thereof.

Transfer of Personal Information

The central competent authority may restrict the international transfer of personal data by the data controller which is not a government agency if:

- Where it involves a major national interest;
- An international treaty or agreement specifies otherwise;
- Where the country receiving personal information lacks proper regulations that protect personal information and that might harm the rights and interests of the data subjects; or
- Where the international transfer of personal information is made to a third country through an indirect method in order to evade the provisions of the PDL.

Security of Personal Information

A company should adopt proper security measures (both technical and organizational) to prevent personal information from being stolen, altered, damages, destroyed or disclosed. The central competent authority may request the company to set up a plan for the security measures of the personal information file or the disposal measures for the personal information after termination of business.

Breach Notification

Where personal information is stolen, disclosed, altered or infringed in other ways due to the violation of the PDPL, the company should notify the individual after due inquiry.

Enforcement

Under the PDPL, a company should be liable for damages and compensation caused by illegal collection, processing and using of personal information. Fines and incarceration vary depending on the severity of the violation.

LVII. Thailand

At present, Thailand does not have any general statutory law governing data protection or privacy. Recently, Thailand proposed the Personal Information Protection Act, but there is no clear indication when or if the draft will ultimately be enacted into binding law.

LVIII. Turkey

Law on the Protection of Personal Data, No. 6698 (2016)

Personal information is protected by the Law on the Protection of Personal Data No. 6698 dated April 7, 2016 (“LPPD”).

Personal Information

Personal information is defined as any information relating to an identifiable natural person. Sensitive personal data is defined as personal data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, clothing, membership of associations, foundations or trade unions, information related to health, sex life, previous criminal convictions and security measures, and biometric and genetic data.”

Registration of Personal Information

The LPPD, a company is required to enroll in the Registry of Data Controllers before proceeding with data processing. If a non-resident, a company shall enroll in the registry through a representative they assign in Turkey. Administrative fines of between TRY 20,000 and TRY 1,000,000 may be imposed on a company breaching obligations regarding the Registry.

Data Protection Officers

The LPPD does not require the appointment of a data protection officer.

Collection and Processing of Personal Information

The LPPD makes it mandatory to comply with certain principles while collecting and processing personal information. Personal information must be:

- Processed fairly and lawfully;
- Accurate and up to date;
- Processed for specific, explicit and legitimate purposes;
- Relevant, adequate and no excessive; and
- Kept for a term necessary for purposes or for a term prescribed in relevant laws for which the data have been processed.

A company must obtain explicit consent of the individual in order to collect and process personal information. However, the LPPD stipulates certain exceptions where consent is not required, and they are:

- Processing is expressly permitted by law;

- Processing is necessary for protection of the life or physical integrity of the individual or third-party, where the individual is not physically or legally capable of giving consent;
- Processing personal information of the contractual parties is necessary for the conclusion or performance of a contract;
- Processing is mandatory for the data controller to perform a legal obligation;
- Personal information has been made public;
- Processing is necessary in order to assign, use or protect a right; or
- Processing is necessary for the legitimate interests the company and this does not damage the rights of the individual.

Processing of sensitive personal information without explicit consent of the individual is generally forbidden.

Deletion, Destruction or Anonymization of Personal Information

The Regulation on Deletion, Destruction or Anonymization of Personal Information was published on October 28, 2017 and entered into force on January 1, 2018. Pursuant to the Regulation, data controllers are required to prepare a personal data processing inventory and a personal data storage and destruction policy (“Policy”).

Transfer of Personal Information

Personal information shall not be transferred without obtaining the explicit consent of the individual, except under the following circumstances:

- Processing is expressly permitted by law;
- Processing is necessary for protection of the life or physical integrity of the individual or third-party, where the individual is not physically or legally capable of giving consent;
- Processing personal information of the contractual parties is necessary for the conclusion or performance of a contract;
- Processing is mandatory for the data controller to perform a legal obligation;
- Personal information has been made public;
- Processing is necessary in order to assign, use or protect a right; or
- Processing is necessary for the legitimate interests the company and this does not damage the rights of the individual.

Personal information shall not be transferred abroad without obtaining the explicit consent of the individual, except under the above circumstances and:

- If the foreign country to whom personal information will be transferred has an adequate level of protection;
- In case there is not an adequate level of protection, if the data controllers in Turkey and abroad commit, in writing, to provide an adequate level of protection and the permission of the Board exists.

Security of Personal Information

Under the LPPD, a company is required to ensure that appropriate technical and organizational measures are taken to prevent all illegal processing and to ensure the data is not destroyed, lost, amended, disclosed or transferred without authority. Such measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in related to the risk. Additionally, a company has to carry out the necessary inspections on its own institution or organization in order to ensure the implementation of the LPPD.

Breach Notification

There is no general breach notification obligation under the LPPD. However, in the event that personal information is obtained by others, a company must notify the Personal Data Protection Board as soon as possible.

Enforcement

The LPPD imposes custodial sentences for the unlawful processing of data. The LPPD introduces administrative fines of up to TRY 1,000,000 for those who act contrary to the requirements or rules.

LIX. UAE – Dubai

Data Protection Law, DIFC Law No. 1 (2007), DIFC Law No. 5 (2012)

The Dubai International Financial Centre (“DIFC”) implemented DIFC Law No. 1 of 2007 Data Protection Law in 2007, which was subsequently amended by DIFC Law No. 5 of 2012 Data Protection Law Amendment Law (“DPL”).

Personal Information

Personal information is any data referring to an identifiable person, *i.e.* a living person who can be identified, directly or indirectly, in particular by reference to an identification number or more factors specific to his biological, physical, biometric, physiological, mental, economic, cultural or social identity.

Sensitive personal information is data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal records, trade-union membership and health or sex life.

Data Protection Officers

Not required under the DPL.

Collection and Procession of Personal Information

A company shall ensure that the personal information which they process is:

- Processed fairly, lawfully and securely;
- Processed for specified, explicit and legitimate purposes in accordance with the individual's rights and not further processed in a way incompatible with those purposes or rights;
- Adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed;
- Accurate and, where necessary, kept up to date; and
- Kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal information was collected or for which they are further processed.

A company may collect and process personal information when any of the following conditions are met:

- The individual has given written consent;
- Processing is necessary for the performance of a contract to which the individual is a party or in order to take steps at the request of the individual prior to entering into a contract;
- Processing is necessary for compliance with any legal obligation to which the company is subject;
- Processing is necessary for the performance of a task carried out in the interest of the DIFC;
- Processing is necessary for the purposes of the legitimate interest pursued by the company or by the third party or parties to whom the personal information is disclosed, except where such interests are overridden by compelling legitimate interests of the individual relating to the individual's particular situation.

A company may collect and process sensitive personal information when any of the following (relevant) conditions are met:

- The individual has given written consent;
- Processing is necessary for the purposes of carrying out the obligations and specific rights of the company;
- Processing is necessary to protect vital interest of the individual or of another person where the individual is physically or legally incapable of giving his consent;
- Processing is necessary for compliance with any regulatory or legal obligation to which the company is subject;
- Processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where the personal information is processed by a health professional subject under national laws or regulations established by national competent bodies to the obligations of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Transfer of Personal Information

A company may transfer personal information abroad if the personal information is being transferred to a recipient in a jurisdiction that has laws that ensure an adequate level of protection. An adequate level of protection is when the level of protection in that jurisdiction is acceptable pursuant to the DPR or any other jurisdiction approved by the Commissioner of Data Protection (“CDP”).

In the absence of an adequate level of protection, a company may transfer personal information abroad if:

- CDP has granted a permit or written authorization;
- The individual has given written consent;
- Transfer is necessary for the performance, or conclusion of a contract between the individual and company;
- Transfer is necessary or legally required on grounds important to the interest of the DIFC;
- Transfer is necessary to protect the vital interests of the individual;
- Transfer is necessary for compliance with legal obligations.

Security of Personal Information

A company must implement appropriate technical and organizational measures to protect personal information against willful, negligent, accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing.

Breach Notification

In the event of a breach, a company must inform the CDP of the incident as soon as reasonably practicable.

Enforcement

The CDP oversees the enforcement of the DPL. A company that fails to comply with a direction of the CDP may be subject to fines and liable for payment of compensation.

An individual who suffers damage by reason of any contravention by a company of any requirement in the DPR or regulation may apply to the court for compensation from the company for that damage.

LX. Ukraine

Law of Ukraine, No. 2297-VI (2010), as amended in (2012), No. 5491-VI, No. 383-VII (UA)

The collection and processing of personal information is governed by the Law of Ukraine No. 2297 VI, as amended in 20 November 2012 No. 5491-VI and 3 July 2013 No. 383-VII.

Personal Information

Personal information is defined as data or an aggregation of data on an individual who is identified or can be precisely identified. Though not defined as sensitive personal information, there is a general prohibition to process personal information with regard to racial or ethnic origin, political, religious ideological convictions, participation in political parties and trade unions, accusation in criminal offenses or conviction to criminal punishment as well as data relating to health or sexual life of an individual.

Registration of Personal Information

A company must notify the Commission of Human Rights (Ombudsman) about personal information processing which is of particular risk to the rights and freedoms of individuals within thirty working days from commencement of such processing. The following types require notification:

- Racial, ethnic, national origin;
- Political, religious ideological beliefs;
- Participation in political parties and/or organizations, trade unions, religious organizations or civic organization of ideological direction;
- State of health;
- Sexual life;
- Biometric data;

- Genetic data;
- Bringing to criminal or administrative liability;
- Application of measures as part of pre-trial investigation;
- Any investigative procedures relating to an individual;
- Acts of certain types of violence used against an individual; and
- Location and/or route of an individual.

The notification procedure shall contain the following:

- Information about the owner of personal data;
- Information about the processors of personal data;
- Information on the composition of personal data being processed;
- The purpose of personal data processing;
- Categories of individuals whose personal data are being processed;
- Information on third parties to whom the personal data are transferred;
- Information on cross-border transfers of personal data;
- Information on the place (address) of processing of personal data; and
- General description of technical and organizational measures taken by personal data owned in order to maintain the security of personal information.

Data Protection Officers

Legal entities shall establish a special department or appoint a responsible person to organize the work related to the protection of personal information during the processing thereof. There are no requirements for the data protection officer to be a citizen or a resident in Ukraine. However, if he or she is a foreign citizen under the general rule, a work permit must be obtained for him or her to hold such position.

Collection and Processing of Personal Information

The Data Protection Law provides for a requirement of obtaining the consent of individuals on processing their personal information. The consent of an individual shall mean the voluntary expression of will of the individual to permit the processing of personal information for the determined purposes, expressed in writing or in some other form which allows the owner or processor of the personal information to make a conclusion that a consent has been granted.

As a general rule, an individual shall be informed, at the moment of collection of their personal data, of:

- The owner of their personal information;
- Composition and content of their personal information being collected;
- Their rights;
- Purpose of their personal information collection; and
- The persons to whom their personal information will be transferred.

Transfer of Personal Information

Personal information may be transferred to a foreign country only on condition of ensuring an appropriate level of protection of personal information by the respective state. The list of states ensuring an appropriate level of protection will be determined by the Cabinet of Ministers of Ukraine.

Personal information may be transferred abroad based on one of the following grounds:

- Unambiguous consent of the individual;
- Abroad transfer is needed to enter into or perform a contract between the personal information owner and a third party in favor of the individual;
- Necessity to protect the vital interests of the personal data subjects;
- Necessity to protect public interest, establishing, fulfilling and enforcing of a legal requirement; or
- Appropriate guarantees of the personal data owner as regards non-interference in personal and family life of the personal data subject.

Security of Personal Information

A company shall take appropriate technical and organizational measures to ensure the protection of personal information against unlawful processing, including against loss, unlawful or accidental elimination, and also against unauthorized access. A company shall determine a special department or a responsible person to organize the work related to the protection of personal information during the processing thereof.

Personal information irrespective of the manner of its storage shall be processed in the way which makes unauthorized access to the data by third persons impossible.

With the purpose of maintenance of security of personal data, technical security measures shall be taken which would exclude the possibility of unauthorized access to personal data being processed

and ensure proper work of technical and program complex through which the processing of personal data is performed.

Additionally, the Data Protection Law requires establishing a structural unit or appointing a responsible person within the personal data owners/processors processing the personal information which is of particular risk to the rights and freedoms of individuals. Such structural unit or responsible person shall organize the work related to protection of personal information during the processing thereof.

Breach Notification

There is no requirement to report security breaches or losses.

Enforcement

A violation of the Data Protection Law may result in civil, criminal and administrative liability.

LXI. United Kingdom

Data Protection Act, 2018, c.12 (U.K.)

The GDPR came into force in the United Kingdom on May 25, 2018, on which date the UK was still a member of the European Union. The United Kingdom prepared a new national data protection law, the Data Protection Act of 2018, which also came into force on May 25, 2018. This law is substantially similar to the GDPR.

Conclusion

The protection of consumer information is under a global microscope as this information becomes more readily available. To avoid civil and criminal penalties, the implementation of a comprehensive compliance program is vital for any company collecting and retaining personal information. We hope you find the 2019 Data Privacy Compendium helpful when beginning to develop your compliance strategy.