Google Cloud

Learn more about data protection and privacy regulations

So far, you've learned that there are many laws and regulations that focus on data protection and privacy. These laws and regulations can apply to different industries, as well as different geographical areas. In this reading, you'll learn more about the data privacy and protection aspects of the the following:

- General Data Protection Regulation (GDPR)
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- California Privacy Rights Act (CPRA)
- Gramm-Leach-Bliley Act (GLBA)
- Children's online privacy Privacy Protection Rule (COPPA)
- Federal Trade Commission (FTC) Act
- Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule

Please note, the following reading should not be considered legal advice.

General Data Protection Regulation (GDPR)

The GDPR is a comprehensive data protection law that applies to processing of personal data by organizations (known as either "data controllers" or "data processors") that are:

- Established in the EU (regardless of whether the personal data is processed in the EU), and/or
- Not established in the EU, but that offer goods and services to individuals in the EU or monitor the behavior of individuals in the EU.

It requires data controllers to have a legal basis for processing personal data about individuals (known as "data subjects"), and gives data subjects various rights in relation to personal data processed about them.

These rights include:

1. The right to be informed (transparency)
2. The right of access to personal data
3. The right to rectification of personal data
4. The right to erasure of personal data
5. The right of restriction of processing of personal data

6. The right to data portability
7. The right to object to processing of personal data
8. Rights in relation to automated decision making, including profiling

The GDPR contains a number of obligations for data controllers and data processors, including a requirement to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Technical measures could include e.g. pseudonymisation and encryption. Organizational measures could include e.g. employee data protection training, internal policies on e.g. data handling, and limiting access to personal data to only those employees in your organization who need it.

And, on the topic of security, data controllers must report personal data breaches to their data protection regulator (known as the "supervisory authority") without undue delay and within 72 hours of becoming aware of the breach, where feasible; unless the breach is unlikely to result in a high risk to individuals. The controller must also notify data subjects affected by the breach without undue delay, where it is likely to result in a high risk to them.

Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA applies to private sector organizations across Canada that collect, use, or disclose personal information in commercial activity. According to PIPEDA, organizations must follow these 10 fair information principles:

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure, and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

California Privacy Rights Act (CPRA)

CPRA is the most comprehensive data privacy law among U.S. states, and is modeled after GDPR. CPRA includes things like obligations on service providers and businesses, and rights given to users that allow them to correct inaccurate information, know categories and specific pieces of personal information, and delete data that was collected about them by a business.

Gramm-Leach-Bliley Act (GLBA)

The GLBA regulates how US financial institutions collect and share non-public personal information of “consumers”: individuals who obtain financial services for personal, family, or household use. The GLBA requires financial institutions to protect both the privacy and security of this information.

Children’s Online Privacy Privacy Protection Rule (COPPA)

COPPA regulates the privacy of children online. It includes certain requirements for the information that online services and websites can collect and share about children under 13 years old.

Federal Trade Commission (FTC) Act

The FTC Act regulates unfair or deceptive trade practices, including those that violate data privacy laws.

Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively, “PHI”) and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Privacy Rule requires appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without an individual’s authorization. The Rule also gives individuals rights over their protected health information, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their protected health information in an electronic health record, and to request corrections.

Key takeaways

As a cloud security analyst, it’s important that you’re familiar with data protection and privacy laws, like GDPR, PIPEDA, CPRA, and HIPAA. These laws help to ensure that organizations are protecting user data and are also compliant in protecting the data privacy rights of users.

Resources for more information

Review these resources for more information about the laws you learned about in this reading:

- PIPEDA provides more detailed information on Canadian data privacy regulations.
- Learn more about GDPR's technical and organizational measures for data protection.