**Data Protection Laws and Mitigating Impacts of Data Breaches**

It’s helpful to understand the legislation in place to protect you from unlawful processing of your private information. Understanding personal rights and legal recourses can help lessen the impact of potential data breaches.

**Data Protection Legislation**

**US Privacy Act of 1974**

Protect consumers against unfair or deceptive practices and to enforce federal privacy and data protection regulations.

For more information: <https://www.ftc.gov/system/files/documents/federal_register_notices/2018/05/p072104_-_data_breach_routine_use_sorn_-_pub_frn.pdf>

**General Data Protection Regulation (GDPR)**

The GDPR’s primary aim is to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

For more information: <https://gdpr-info.eu/>

**California Consumer Privacy Act (CCPA)**

2018 state statute intended to enhance privacy rights and consumer protection for residents of California.

For more information: <https://oag.ca.gov/privacy/ccpa>

**ISO/IEC 27001**

The aim of ISO/IEC 27001 is to help organizations make the information assets they hold more secure.

For more information: <https://www.iso.org/news/2013/08/Ref1767.html>

**Sector Specific Data Protection in the US**

There are many sector specific statutes that focus on collected data.

**Health Insurance Portability and Accountability Act (HIPPAA)**

Stipulate how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft.

For more information: <https://www.hipaaguide.net/hipaa-for-dummies/>

**Gramm-Leach-Bliley Act (GLBA)**

Financial institutions must provide their clients a privacy notice.

For more information: <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act>

**Children’s Online Privacy Protection Act (COPPA)**

Applies to the online collection of personal information by persons or entities under U.S. jurisdiction about children under 13 years of age including children outside the U.S., if the company is U.S.-based.

For more information: <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0>

**Principles of Responsible Data Collection and Processing**

As a result of this legislation there are general principles that have arisen as a framework for data protection best practices.

**Transparency**

Businesses are generally encouraged to provide clear and standardized privacy information.

For more information: <https://www.ftc.gov/system/files/documents/federal_register_notices/2018/05/p072104_-_data_breach_routine_use_sorn_-_pub_frn.pdf>

For more information: <https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa#:~:text=There%20is%20no%20single%20principal,Code%20%C2%A7%2041%20et%20seq>.)

**Purpose Limitation**

The FTC recommends privacy-by-design practices.

For more information: <https://www.ftc.gov/system/files/documents/federal_register_notices/2018/05/p072104_-_data_breach_routine_use_sorn_-_pub_frn.pdf>

For more information: <https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa#:~:text=There%20is%20no%20single%20principal,Code%20%C2%A7%2041%20et%20seq>.)

**Retention**

The FTC recommends privacy-by-design practices that implement reasonable restrictions on the retention of data.

For more information: <https://www.ftc.gov/system/files/documents/federal_register_notices/2018/05/p072104_-_data_breach_routine_use_sorn_-_pub_frn.pdf>

For more information: <https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa#:~:text=There%20is%20no%20single%20principal,Code%20%C2%A7%2041%20et%20seq>.)

**Privacy By Design**

Data privacy should be considered at the beginning of security planning, not after.

For more information: <https://www.varonis.com/blog/privacy-design-cheat-sheet/>