Overview of U.S. Privacy Legislation

Understanding and complying with all levels of privacy regulation – federal, state, county and municipal – is an essential part of doing business to protect both yourself and your customers. Here is our brief overview at the federal level to get you started.

1. The Fair & Accurate Credit Transaction Act (FACTA)

- Rights of consumers to access their credit information
- Rules on accuracy and privacy of consumer financial information contained or derived from a consumer report
- Provisions to help protect against identity theft
- Obligations to establish and monitor policies and procedures for the secure destruction of consumer information – to prevent unauthorized access and use

Penalties:

Up to $1,000 for actual damages plus punitive damages and the costs of action.

2. Gramm-Leach-Bliley Act (GLBA)

- Rules to protect the privacy of consumer information held by any business that provides financial products or services
- Rules on accuracy and privacy of consumer financial information contained or derived from a consumer report
- Obligations to provide privacy notices regarding information sharing practices
- Rights of consumers to limit some sharing of their information by financial institutions

Penalties:

Financial institutions as well as officers and directors can be fined, or imprisoned, depending on whether the offence was committed under the GLBA Act, Title 18 of the United States Code and/or the Federal Deposit Insurance Act (FDIA).

Individual officers/directors can be fined up to $1,000,000.

3. Sarbanes-Oxley Act (SOX)

- Rules for publicly-traded companies, and their relevant service providers, on the strict financial reporting requirements for increased corporate responsibility
- Rules on accuracy and privacy of consumer financial information contained or derived from a consumer report
- Obligations for companies and their auditors to maintain information and records management policies and procedures
- Requirements for secure document retention and destruction – to better protect against corporate and accounting fraud

Penalties:

Fines and/or imprisonment of up to 20 years depending on the severity of the infraction by the company or individual.

4. HIPAA & HITECH Acts

- Rules for adequate safeguards to protect the privacy and security of Protected Health Information (PHI) by health care service providers (or "Covered Entities") and their business associates
- Obligations to ensure the confidentiality of PHI, whether hardcopy or electronic records, up to and including their secure destruction
- Circumstances and requirements for public notification after a breach of PHI

Penalties:

Based on a tiered range of minimum civil monetary penalties according to the infringement, to a maximum of $1.5 million for all violations of an identical provision.

For more information:

Federal Trade Commission – **ftc.gov**
U.S. Department of Health & Human Services – **hhs.gov/ocr/hipaa**
Economic Espionage Act – **economicespionage.com/EEA**
U.S. Department of Commerce – **export.gov/safeharbor**
U.S. Securities & Exchange Commission – **sec.gov**
U.S. Department of Justice – **justice.gov**

Shred-it®

5. Economic Espionage Act (EEA)

- Protection of actual, or potential, economic value that is derived from trade secrets
- Classifications of trade secret information – types and formats
- Requirements of owner to be able to show that adequate protective measures were taken in order for the information to be defined as a trade secrets

Penalties:

Two categories for theft of trade secrets –

1) for benefit of a foreign entity or
2) causes injury to owner.

Organizations face maximum fines of $5 – $10 million (or twice the loss/gain, if greater). Individuals can be imprisoned for 10 – 15 years and/or fined $250,000 – $5 million (or twice the loss/gain, if greater).

6. Safe Harbor Framework

- Self-regulatory and voluntary framework based on seven principles concerning information management and the secure protection of personal information
- Requirements for annual self-certification to be eligible to receive data from European countries, under the EU Directive on Data Protection
- Options for organizations to join a self-regulatory privacy program or develop their own privacy policy to conform to the program

Penalties:

Dispute resolution bodies can suspend participants from their privacy program or issue injunctive orders.

Failure to comply with self-imposed regulations is also actionable under federal or state law as unfair or deceptive acts. Enforcement of safe harbor principles can lead to civil penalties – e.g. $16,000 per day by the Federal Trade Commission.

7. Patriot act

- Rules to expand the ability of law enforcement to conduct surveillance and capture information during foreign intelligence and counter-terrorism investigations
- Requirements for companies to produce information quickly for law enforcement bodies
- Obligations for financial institutions to have adequate procedures to identify customer account information as well as verify and maintain records on a customer's identity

Penalties:

Failure to produce information quickly for law enforcement agencies with a court order may lead to the organization being held in contempt. Section 215 does not specifically detail any additional legal repercussions and penalties.

How Shred-it® can help

Secure Document and Hard Drive Destruction

- Secure end-to-end chain of custody
- Certificate of Destruction after every service
- Tailored solutions to your organization's needs

Advice and Expertise

- Trained experts in information security
- A Free Security Risk Assessment is performed on-site
- Helpful resources available at shredit.com