Infographic

Financial Data Regulations to Watch

Cybersecurity teams at financial service firms have to watch regulatory requirements, not just cyber criminals. Know what is required of your IT systems.

Gramm-Leach-Bliley

Designed to protect consumer financial privacy through non public identifiable information (PII). Companies offering consumer financial services must inform consumers about how financial information is shared and safeguarded. **Consumers have the right to opt out of having their information shared, and data reuse and disclosure are limited.**

Sarbanes-Oxley

Enacted to protect investors from fraudulent financial reporting. Accountants, auditors and corporate officers have strict recordkeeping requirements, and senior corporate officers must certify that financial statements comply disclosure requirements of the SEC. **Specific internal controls and reporting methods are also mandated, and the length of time electronic documents must be stored.**

General Data Protection Regulation

Passed to safeguard EU citizens living anywhere in the world, GDPR requires that organizations inform customers and visitors about the manner of data collection and use. Explicit consent must be given for data gathering, and any PII must be either anonymized or pseudo-anonymized. **Consumers also must be notified of data breaches, and they have the right to request data removal. Applies to company employees also.**

California Consumer Privacy Act

A Californa version of GDPR, the CCPA mandates that consumers have the right to know what information a business is collection about them and how it will be used. They also can require deletion of PII collected, opt out of the sale of this information and not be discriminated against for these actions. **Privacy rights and practices must be given to consumers as well.**

23 NYCRR Part 500

This New York State regulation specifies that national security companies must use technical and procedural tools to continuously monitor shared data and systems to evaluate and address security risks. **Exemption exist for small businesses.**

Personal Information Protection and Electronic Documents Act

A Canadian regulation that requires organizations that conduct business in the country to have privacy policies in place. Financial institutions must obtain consent from consumers before collecting, using or disclosing any PII, and must provide consumers with the right of access to that information. **Companies are required to safeguard information and limit retention of PII.**

Payment Card Industry Data Security Standard

PCI-DSS is a compliance standard for any entity dealing with the processing, transmission and storage of credit card information. **Standards include building, maintaining and regularly testing secure networks/systems, protecting cardholder data, ensuring proper vulnerability mitigation, assigning unique user IDs, and tracking or restricting access to network resources and data.**

Free Download

How to Identify and Classify Sensitive Data. Get the guide that walks you through the steps of tagging and classifying data.

FREE GUIDE