coretelligent

THE POWER OF IT™

A GUIDE TO UNDERSTANDING DATA SECURITY & DATA PRIVACY COMPLIANCE

ARE YOU CONFIDENT IN YOUR DATA PRIVACY COMPLIANCE?

In today's digital age, data privacy has become a top priority for individuals and organizations alike. With data breaches and privacy violations making headlines all too frequently, it's crucial that companies take data privacy compliance seriously. However, many businesses struggle to navigate the complex web of regulations and standards in the world of data privacy.

Are you confident that your organization is fully compliant with the relevant data privacy regulations? This guide aims to provide a comprehensive overview of the primary data privacy reguirements. With the potential financial, legal, and reputational risks associated with non-compliance, it's never been more critical to prioritize data privacy and ensure that you and your organization are doing everything possible to protect sensitive information.

HOW DO I KNOW WHAT REGULATIONS TO FOLLOW?

There are three main factors in determining what privacy regulations apply to your business.

INDUSTRY

Some industries are required to follow specific regulations depending on their sector.

LOCATION

Various countries and states have implemented disparate sets of privacy laws.

SIZE

Some regulations only apply to companies that fall within certain size ranges.

Each of these factors can have an impact on what regulations apply to your business. For example, if you are a financial services firm operating in the United States, you may be subject to certain regulations and not others.

WHAT ARE THE MAIN DATA PRIVACY REGULATIONS BY INDUSTRY?

- **ALL INDUSTRIES**

  GDPR
  CCPA/CPRA
  NY Shield Act
  & Other State Regulations

- **FINANCIAL SERVICES**

  SOX
  SEC
  FINRA

- **LIFE SCIENCES**

  HIPAA
  HITRUST
  SOX

GDPR

The General Data Protection Regulation (GDPR) is a set of European Union regulations implemented to protect consumers' privacy and personal data in the E.U. Companies must now be more transparent about how they use an individual's data, giving user the right to know what data is being collected, the "right to be forgotten," and other more. Even though the intent is to safeguard consumers' data privacy in the E.U., it also applies to companies outside that region that collect consumer data from individuals residing within the region.

CCPA/CPRA

The California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) are a set of privacy laws that provide California residents with certain rights over their personal data. The CCPA requires companies to provide consumers privacy notices and the right to opt out of certain data processing. The CPRA expands on the laws set out in the CCPA. Both apply to any company that does business in California and collects or processes the data of any California residents.

SOX

The Sarbanes-Oxley Act (SOX) is a federally-mandated law that requires publicly traded companies in the U.S. to establish financial reporting standards, including safeguarding data, tracking attempted breaches, logging electronic records for auditing, and proving compliance. It also requires companies to set up internal controls to help protect against fraud and data manipulation, including ensuring that any personal data collected for business purposes is secure.

NY SHIELD ACT

The Shield Act is a set of state laws to protect and secure the data of New York residents. The Act applies to companies that conduct business in N.Y. or collect data from N.Y. residents. It requires organizations to implement reasonable cybersecurity measures that include technical, administrative, and physical safeguards to protect nonpublic information. Other states have implemented or are planning to implement data privacy laws that businesses must comply with if they do business in those states or collect and process data from residents.

SEC

The Securities and Exchange Commission (SEC) is a U.S. agency responsible for overseeing and regulating the securities markets and protecting investors. Among the many areas the agency oversees, the SEC enforces laws like the Sarbanes-Oxley Act as well as implements and enforces its own compliance standards for SEC-registered investment companies via the Division of Examinations.

FINRA

The Financial Industry Regulatory Authority (FINRA) is a self-regulatory organization in the U.S. that oversees broker-dealers and their activities, including ensuring the security of customer data. Broker-dealers are companies that engage in the business of trading securities for their account or on behalf of their customers. FINRA has outlined what it expects from firms to protect customers' personal information and guard against cyber threats.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. federal law designed to protect the privacy of patients' protected health information (PHI). HIPAA requires healthcare providers, insurance companies, and companies that collect PHI to implement specific security standards and procedures for protecting such data from unauthorized access or use. The HIPAA Privacy and Security Rules are enforced by the Office for Civil Rights (OCR).

HITRUST

HITRUST is a security framework from the Health Information Trust Alliance (HITRUST) that addresses many of the data privacy requirements outlined in HIPAA. While HIPAA is a law created by lawyers and lawmakers, HITRUST is a framework created by security industry experts which includes aspects of HIPAA. It enables organizations to demonstrate compliance with HIPAA requirements. It is just one approach that can be taken to gain compliance but is not necessarily a requirement for compliance.

WHAT TYPES OF REQUIREMENTS DO REGULATIONS ADDRESS?

Collection

The regulations for data collection guide businesses on when and how they can collect information about consumers. These regulations may also require businesses to notify individuals if their data is being collected.

Event Notifications

Businesses are required to follow specific actions in case of a data breach, which include informing relevant agencies and customers, keeping a record of details related to the breach, and implementing measures to prevent a similar breach from occurring again.

Access

The regulations for data access provide instructions on how to manage internal access to information and determine the levels of access for consumers.

Storage

Data storage regulations define the requirements for securely storing data. The regulations vary in specificity and address aspects such as the duration of data retention and the security measures necessary for your storage system.

End-user Training

Businesses are required to provide training to employees in order to protect data. Typically, all employees must undergo ongoing training to comply with the regulations.

WHAT'S THE DIFFERENCE BETWEEN DATA PRIVACY AND DATA SECURITY?

Data privacy and data security are closely related concepts, but there is an important distinction between the two.

Data privacy focuses on how data is collected, used, shared, and protected by organizations. It includes laws like the General Data Protection Regulation (GDPR) that protect personal information.

Data security is a set of strategies and measures that businesses use to protect their data from unauthorized access or misuse. It includes technologies like authentication and processes such as data backup and user access controls. The NY Shield Act addresses both data privacy and security.

Choosing the right IT partner can make all the difference in meeting your firm's business goals and mitigating risk. **Coretelligent** has extensive experience supporting clients with their specific cybersecurity and compliance requirements.

With our white-glove service approach, years of experience, industry specialization, and a range of technology solutions, we can help your firm fully align technology with your risk profile and business goals. In addition, as a full life-cycle provider, we also deliver IT planning and strategy, 24/7/365 support, cloud sloutions, cybersecurity, digital transformation, backup and disaster recovery, and more.

Learn how **Coretelligent** can help your firm solve compliance by visiting **www.coretelligent.com** or calling **855.841.5888** to speak to our experts.

ABOUT CORETELLIGENT

As a leading provider of comprehensive managed IT, cybersecurity, digital transformation, DevOps, IT strategy, and more, Coretelligent enables organizations to seamlessly power and grow their businesses. Founded in 2006 and led by world-class technology experts, Coretelligent's core services are utilized by top-tier organizations in the financial services, life sciences, legal, and technology industries, among others. Coretelligent's headquarters is in Needham, MA, with strategic offices located in New York City, Atlanta, Norwalk, Scarborough, and the San Francisco Bay area; with expanded support locations in Dallas, Los Angeles, Philadelphia, Tampa, Washington, DC, and West Palm Beach.