Regulations and compliance

Due to global connectivity and the use of cloud services, to store sensitive data and personal information, both inherent and residual risks are increasing. With the rise of cybercrimes and data breaches, organizations must be protected from all types of theft and damage and defend themselves from data breach campaigns. Sophisticated cybercriminals combined with the widespread poor configuration of cloud services mean the organization is increasingly vulnerable to cyberattacks and data breaches.

The Coro platform helps businesses protect their data and stay compliant with many of today's privacy and security regulations. We've put together some information to help you understand the regulations relevant to your business, and how Coro helps exactly.

The following table provides a high-level overview of each of the regulations, and a link to additional information:

Regulation	Overview	Governs these parties	Enforced by
ADPPA	Governs how companies across different industries treat consumer data	All organizations that treat consumer data. It applies to most entities, including nonprofits and common carriers	The Federal Trade Commission
CCPA	Gives consumers more control over the personal information that businesses collect about them	All organizations processing information on California residents or doing business in California	The Office of the Attorney General (OAG)
CJIS	Keeps networks aligned when it comes to data security and encryption and ensures that sensitive criminal justice intel is locked down with the continuity of information protection	All personnel who have unescorted access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process, or transmit unencrypted CJI	The Criminal Justice Information Services Division
COPPA	Protects the privacy and personal information of children under the age of 13 who use online services.	All websites, online services, and mobile apps	The Federal Trade Commission

Regulation	Overview	Governs these parties	Enforced by
CPA	Protects consumers in their online activities and gives people more control over their personally identifiable information, including making inquiries and requests to data controllers	All organizations processing information on Colorado residents or doing business in Colorado	The Office of the Attorney General (OAG)
CPRA	Regulates how businesses collect and use data about consumers in California	All organizations processing information on California residents or doing business in California	The Office of the Attorney General (OAG) or the California Privacy Protection Agency
CTDPA	Obligates data controllers to fulfill certain basic data protection principles, such as data minimization and the purpose limitation	All legal entities conducting business in Connecticut or delivering products or services targeted to Connecticut residents	The Office of the Attorney General (OAG)
FERPA	Protects the privacy of student's educational records	All educational institutions that receive funding from the U.S. Department of Education	U.S. Department of Education. Specifically, the Family Policy Compliance Office (FPCO)
FISMA	Aims to reduce the potential risk of unauthorized data use, to develop, document, and implement an information security and protection program disclosure, or loss, no matter where along the chain it might originate	US federal agencies that provide services or receive grant money	The Department of Homeland Security
GDPR	Governs businesses to protect those business's systems from any potential attacks, and to protect their consumers' data, with stricter rules surrounding the handling of personal data	All organizations which target or collect personal data related to European Union residents	The European Commission, works with each EU Member State, and designates an independent public authority
GLBA			

Regulation	Overview	Governs these parties	Enforced by
	Governs companies that qualify as “financial institutions” to take several affirmative steps in order to prevent the unauthorized collection, use, and disclosure of NPI (Nonpublic Personal information)	All businesses that are significantly engaged in providing financial products or services	The Federal trade commission (FTC)
HIPAA	A series of regulatory standards that outline the lawful use and disclosure of protected health information (PHI)	All organizations that: receive payment for their services and transmit personal or health information for the purposes of treatment, operations, billing, or insurance coverage	The Department of Health and Human Services (HHS), Office for Civil Rights (OCR), the Centers for Medicare and Medicaid Services (CMS), the Federal Drug Administration (FDA), and the Federal Communications Commission (FCC)
ISO 27001 (ISMS)	Helps organizations protect their information in a systematic and cost-effective manner in terms of confidentiality, integrity, and availability	All organizations that store or manage data, IT-based, Health, Government, and public companies	The majority of global companies require their partners and vendors to meet these standards
MIPSA	Requires that every person that owns or licenses personal information about a resident of the Commonwealth must develop, implement, and maintain a comprehensive information security program	All organizations processing information on Utah residents or doing business in Massachusetts	The office of the Attorney General (OAG)
MOCPA	Applies to processing the information on residents or doing business in Maryland or establishing a Workgroup on Online Consumer Personal Information Privacy	All organizations processing information on residents or doing business in Maryland	The office of the Attorney General (OAG)
NYDFS	Ensures the safeguarding of sensitive customer data and to promote the integrity of the information	All insurance companies, banks, and other regulated financial services	The New York State regulators at the

Regulation	Overview	Governs these parties	Enforced by
	technology systems of regulated entities to assess their cybersecurity risks and develop plans to address them proactively	institutions — including agencies and branches of non-US banks licensed in New York	Department of Financial Services
NYPA	Sets forth provisions for companies to manage personal data responsibly and lawfully. Like Europe's GDPR, the NYPA includes lawful processing, consent, and individual rights to name a few	All organizations processing information on residents or those doing business in New York	The office of the Attorney General (OAG)
PCI DSS	Protects credit, debit, and cash card transactions and prevent the misuse of cardholders' personal information	Any business that accepts card payments, including seasonal or small businesses	Visa, Mastercard, AmEx, JCB, and Discover
SOC2	Helps companies determine whether their business partners and vendors can securely manage data and protect the interests and privacy of their clients	All technology service providers or SaaS companies that store or handle client data	The majority of global companies require their partners and vendors to meet these standards
SOX	Lays out a set of requirements for annual audits to assess and protect shareholders in financial & IT public companies by securing their access controlling data management and preventing breaches and fraud. SOX describes a course of action to take in order to show evidence of accurate, secured financial reporting and it provides companies with a way of improving their data security whilst simultaneously helping to restore public confidence, reducing chances of falling victim to a data breach	All publicly traded companies in the USA, as well as any wholly-owned subsidiaries and foreign companies that are both publicly traded and do business with the USA. Any accounting firms that are auditing companies bound by SOX compliance are also, by proxy, obliged to comply	The Securities and Exchange Commission (SEC)
UCPA	Gives consumers substantial control over their personal data, and emphasizes the privacy of children, in particular, providing tools to protect	All businesses that process personal data and data rights for Utah citizens	he office of the Attorney General (OAG)

Regulation	Overview	Governs these parties	Enforced by
	their privacy and control the usage of their personal data		
VCDPA	Enforces the consumer's right to opt-out of having personal data collected, processed, and sold, requiring companies and organizations to obtain prior consent from end-users if they collect or process sensitive personal data.	All websites, companies, and organizations that do business in Virginia, or that produce products or services targeted to residents of Virginia	The office of the Attorney General (OAG)