



Cybersecurity Compliance Guide

CONSUMER
TRANSACTIONS

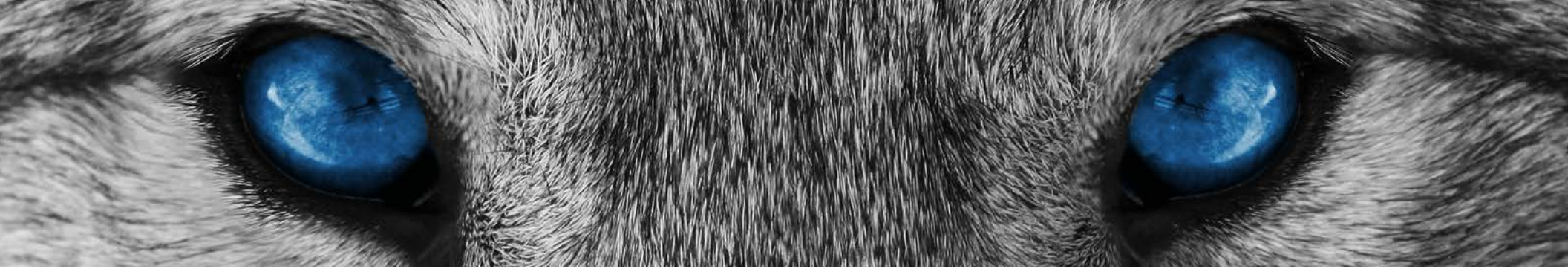
EDUCATION

BANKING

GOVERNMENT


HEALTHCARE

PERSONAL | PREDICTABLE | PROTECTION



CONTENTS

Introduction	3	Healthcare	12
Consumer Transactions	4	▶ Healthcare Insurance Portability and Accountability Act	12
▶ PCI DSS.....	4	▶ Healthcare Information Trust Alliance Common Security Framework	13
Education	5	Location-Specific	14
▶ Family Educational Rights and Privacy Act.....	5	▶ California Consumer Privacy Act.....	14
Banking	7	▶ New York SHIELD Act.....	15
▶ Sarbanes-Oxley Act	7	▶ New York State Department of Financial Services Cybersecurity Regulation	16
▶ Gramm-Leach-Bliley Act.....	8	▶ General Data Protection Rule	17
▶ FFEIC Cybersecurity Assessment	9	▶ Other State Privacy and Cybersecurity Laws	18
▶ Basel III IT Operational Controls.....	9	Next steps	19
Government	10		
▶ NIST 800-171.....	10		
▶ Federal Information Security Management Act	11		



Compliance is an important part of a cybersecurity program. Heavily regulated industries are often a bigger target for cybercriminals because of their highly valuable data (e.g., patient data in healthcare, financial data in banking, identity data in government). The purpose of cybersecurity laws and regulations are to ensure that organizations take the right steps to protect this data. And regardless of what industry you're in, you need to comply with state privacy laws, GDPR, and other regulations that apply to all sectors.

While meeting compliance requirements doesn't guarantee that your organization is secure, it provides you with a solid foundation for security practices. Not to mention that noncompliance may lead to fines and other penalties.

Use this guide as an overview of compliance requirements for your industry and location. We've provided a summary of each rule and key requirements, along with resources for more information.

CONSUMER TRANSACTIONS

Protecting customer data is important for maintaining your brand reputation and customer trust. Regardless of your industry, if you accept debit and credit cards, you are subject to Payment Card Industry Data Security Standards (PCI DSS). This set of standards is developed, maintained, and enforced by the payment card industry, and noncompliance can result in fines.

PCI DSS

Summary

Payment Card Industry Data Security Standards (PCI DSS) are not government regulations but rather a set of industry rules that payment card issuers and financial institutions enforce for merchants and service providers who accept payment cards. The PCI Security Standards Council develops and maintains the standards, which also apply to anyone who stores, processes, or transmits cardholder data. Additionally, there are requirements for software developers and hardware manufacturers of applications and devices used in payment transactions.

Merchants must assess their compliance, remediate vulnerabilities, and report compliance to the respective financial institution or payment card brand.

Key requirements

PCI-DSS has a set of six core objectives, each with specific requirements:

- ▶ Build and maintain a secure network—using a firewall and strong password practices
- ▶ Protect stored cardholder data—including encryption of cardholder data when it's transmitted over open, public networks
- ▶ Maintain a vulnerability management program—using and regularly updating anti-virus and secure apps
- ▶ Implement strong access control measures—including restricted access to data based on roles and unique IDs for those with access
- ▶ Regular monitor and test networks—tracking and monitoring access to networks and data, and regularly testing security
- ▶ Maintain an information security policy—covering both employees and contractors

Who's affected

Entities anywhere in the world that transmit, store, or process cardholder data.

Resources

- ▶ [Arctic Wolf: Simplify PCI DSS Compliance](#)
- ▶ [PCI Security Standards Council: Best Practices for Maintaining PCI DSS Compliance](#)

EDUCATION

K-12 schools and institutions of higher education need to protect the privacy of their student records. All schools funded by U.S. Department of Education programs must comply with the federal Family Educational Rights and Privacy Act, whose aim is to ensure the protection of education records and personally identifiable information (PII). Additionally, most states have their own laws that apply to the education sector.

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT

Summary

The Family Educational Rights and Privacy Act (FERPA) is a federal privacy law that protects students' education records and personally identifiable information from unauthorized disclosure. All schools that receive certain types of U.S. Department of Education funds must comply, and noncompliance can result in loss of the federal funding. Enacted in 1974, FERPA prohibits the disclosure of student records without written consent, with some specific exceptions.

Key requirements

FERPA gives parents of students under 18 specific rights with regards to student records, and those rights transfer to the students when they reach age 18. These rights include the ability to:

- ▶ Inspect the student records maintained by the institution
- ▶ Request the correction of records that they believe are inaccurate
- ▶ Provide written permission for the records to be disclosed

Certain conditions are exempt from the written permission requirement, including organizations conducting studies on behalf of the school, law-enforcement and court entities, and officials conducting audits. Additionally, FERPA allows disclosure without consent of directory information, such as student name, address, and date of birth, but requires institutions to provide parents or eligible students the opportunity to opt out.

Who's affected

In general, educational agencies and institutions that receive funds administered by the U.S. Secretary of Education and provide services or instruction to students, or are authorized to direct and control public educational institutions (with some exceptions).

Resources

- ▶ [U.S. Department of Education: FERPA](#)
- ▶ [EdTech Magazine: FERPA Compliance in the Digital Age – What K-12 Schools Need to Know](#)
- ▶ [Louisiana College: FERPA Best Practices for Electronic Communication](#)

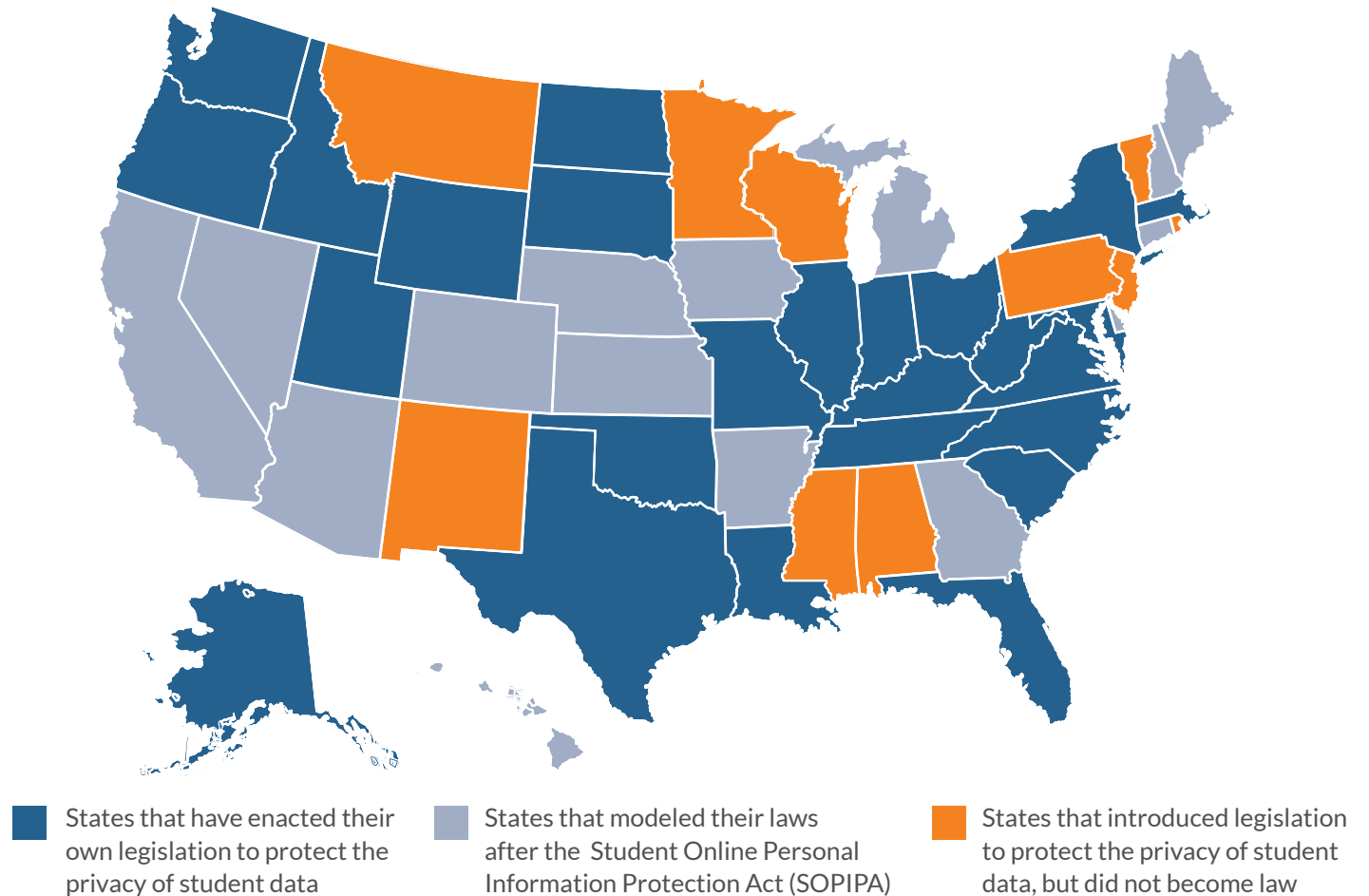
EDUCATION

State laws

At least 40 states have enacted their own legislation to protect the privacy of student data.

More than 20 of them have modeled their laws after California's 2014 Student Online Personal Information Protection Act (SOPIPA), while others have used frameworks such as the Student Data Privacy, Accessibility, and Transparency Act, originally developed by the Foundation for Excellence in Education.

SOPIPA, which came into effect in January 2016, applies to entities that operate websites, online services, and online and mobile apps that are designed and marketed primarily for K-12 educational purposes. It requires these operators to implement reasonable security practices to protect the student data, and prohibits them from sharing the data or using it for advertising for noneducational purposes.



Resources

- ▶ [Parent Coalition for Student Privacy: State Student Privacy Laws](#)
- ▶ [FindLaw: Links to State School Records Privacy Laws](#)

BANKING

The financial sector is heavily targeted by cybercriminals, who typically go where the money is. In response, several government agencies aim to protect consumer information. The Gramm-Leach-Bliley Act enforces the safeguarding of sensitive data for organizations that offer financial products, with penalties including not only fines but also criminal action against individuals. The Federal Financial Institutions Council provides a Cybersecurity Assessment Tool to help mitigate security risks. Additionally, the Sarbanes-Oxley Act requires controls that ensure financial reports are complete and accurate, and the international Basel Committee on Banking Supervision has IT requirements related to data integrity.

SARBANES-OXLEY ACT

Summary

The Sarbanes-Oxley Act of 2002 (SOX) regulates financial practices and corporate governance, and applies to all publicly traded companies as well as accounting firms and other entities that provide financial services to those companies. Its main objective is to protect investors from fraudulent accounting activities. SOX requires the regulated entities to implement internal accounting controls and report the adequacy of those controls to the Securities and Exchange Commission (SEC). Noncompliance can result in fines and other penalties, including criminal liability.

Key requirements

From a cybersecurity perspective, two sections of SOX are particularly relevant:

- ▶ Section 303 requires the chief executive officer and chief financial officer to personally certify that their company's financial reports are accurate and complete, and places responsibility on them for assessing and reporting the effectiveness of the internal controls related to financial reporting
- ▶ Section 404 requires the entity to assess the effectiveness of internal controls and report it annually to the SEC. An outside auditing firm must review this assessment, which includes a comprehensive review of the internal controls. However, SOX doesn't provide guidance around specific controls that must be assessed

Who's affected

All publicly traded companies regardless of size and industry; some provisions also apply to private and nonprofit entities.

Resources

- ▶ [SANS: An Overview of Sarbanes-Oxley for the Information Security Professional](#)
- ▶ [TechTarget: SOX Compliance Checklist](#)

BANKING

GRAMM-LEACH-BLILEY ACT

Summary

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions and other entities that provide financial products—including loans, insurance, and investment advice—to safeguard sensitive data and to explain their information-sharing practices to their customers. The Federal Trade Commission and other federal agencies enforce the GLBA, and noncompliance penalties include fines and criminal charges.

Key requirements

The GLBA has two core components:

1. The Safeguards Rule requires financial institutions protect the consumer information they collect. Requirements include:
 - ▶ Designating an individual or group to coordinate an information security program
 - ▶ Identifying and assessing risks to customer data and evaluating the effectiveness of the existing controls
 - ▶ Implementing, monitoring, and testing a safeguards program
 - ▶ Evaluating the program when changes take place in business operations and other circumstances
 - ▶ Ensuring service providers can maintain the appropriate safeguards
2. The Privacy of Consumer Information Rule (or Privacy Rule) requires regulated entities to inform consumers about their information-collection practices and to explain their rights to opt out. The rule includes requirements for the contents of the notices, delivery methods, and frequency.

Who's affected

Financial institutions, defined as entities of any size that are “significantly engaged” in providing financial products and services, including banks, insurance companies, lenders, auto dealers that offer credit and leasing, payday lenders, professional tax preparers, real estate appraisers, and others.

Resources

- ▶ [FTC: How to Comply with the Privacy of Consumer Information Rule of the Gramm-Leach-Bliley Act](#)
- ▶ [FTC: Complying with the Safeguards Rule](#)

BANKING

FFEIC CYBERSECURITY ASSESSMENT

Summary

The Federal Financial Institutions Council (FFEIC) has released the Cybersecurity Assessment Tool to help banks and credit unions assess and mitigate their cybersecurity risks. The assessment, which is voluntary, maps to the Nation Institute of Standards and Technology (NIST) Framework, which is widely used by all industries as a tool to strengthen cybersecurity posture.

Key requirements

FFEIC guidance applies to federally supervised financial institutions. The FFEIC Cybersecurity Assessment Tool has a twofold objective:

- ▶ To identify the institution's inherent risk profile—includes activities, products, and services in five categories: technologies and connection types, delivery channels, online and mobile products and technology services, organizational characteristics, and external threats
- ▶ To determine the organization's maturity level—focused on five domains: cyber risk management and oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and cyber incident management and resilience

Resources

- ▶ [FFIEC: Cybersecurity Assessment Tool website](#)
- ▶ [Arctic Wolf: Simplify Compliance for FFIEC-NCUA](#)
- ▶ [Arctic Wolf: 5 Steps to Ace the FFIEC Assessment](#)

BASEL III IT OPERATIONAL CONTROLS

Summary

The Basel Committee on Banking Supervision (BCBS) is an international supervisory authority that maintains several standards and voluntary frameworks for financial institutions. Basel III (and Standard 239), in particular, affects IT infrastructure and operations, as it includes principles related to data architecture and IT infrastructure, as well as accuracy and integrity of risk data.

Key requirements

To comply with the BCBS effective risk data aggregation and risk reporting principles, financial institutions must have a robust and resilient IT infrastructure that supports risk aggregation capabilities and risk reporting practices both in normal times and in times of stress or crisis.

Who's affected

Internationally active banks

Resources

- ▶ [BCBS: Principles for Effective Risk Data Aggregation and Risk Reporting](#)
- ▶ [Deloitte: Basil III: Principles for Effective Risk Data Aggregation and Risk Reporting](#)

GOVERNMENT

To protect the security and privacy of its information and systems, some government agencies have cybersecurity requirements for their contractors, including commercial entities and nonfederal agencies. The National Institute for Standards and Technology develops and maintains the requirements, which include NIST 800-171, required by the Department of Defense and others. Contractors may also be subject to the Federal Information Security Management Act.

NIST 800-171

Summary

The National Institute for Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, provides recommendations for cybersecurity standards and data protection for nonfederal entities that serve as federal contractors, including commercial and state or local government organizations. Several federal agencies, such as the Department of Defense and the General Services Administration, mandate compliance with these standards.

Key requirements

Controlled unclassified information (CUI) refers to information that is not classified but is considered sensitive. SP 800-171 includes basic and derived requirements in 14 domains:

- ▶ Access controls (such as limiting access to authorized users)
- ▶ Awareness and training
- ▶ Audit and accountability (such as maintaining system audit logs)
- ▶ Configuration management (for hardware, software, and firmware)
- ▶ Identification and authentication (includes users, processes, and devices)
- ▶ Incident response
- ▶ Maintenance of systems
- ▶ Media protection (both physical and logical controls)
- ▶ Personnel security
- ▶ Physical protection
- ▶ Risk assessment
- ▶ Security assessment
- ▶ System and communications protection (including data transmission)
- ▶ System and information integrity

Who's affected

Commercial businesses and state or local government agencies that serve as federal contractors for certain federal agencies (including the Department of Defense).

Resources

- ▶ [NIST: Special Publication 800-171](#)
- ▶ [Arctic Wolf: Simplify NIST 800-171 Compliance](#)

GOVERNMENT

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

Summary

The Federal Information Security Act of 2002 (FISMA) requires federal agencies to develop, document, and implement an information security program for the data and systems that support the agencies' operations and assets. The requirement also applies to information and systems provided or managed by other sources, such as contractors and nonfederal agencies. Entities funded by certain federal grants, such as educational institutions, may also be required to comply with FISMA.

Key requirements

NIST develops the standards and guidelines for FISMA compliance using a risk-based approach. It uses a framework that includes seven core steps, some of which map to specific NIST Special Publications (SPs):

- ▶ **Prepare:** Conducting the essential activities to help prepare for risk management under the framework
- ▶ **Categorize:** Classifying the information and systems that must be protected
- ▶ **Select:** Establishing the baseline controls for protecting the categorized systems and data
- ▶ **Implement:** Deploying the appropriate controls and documenting them
- ▶ **Assess:** Determining if controls are working correctly and leading to desired outcomes
- ▶ **Authorize:** Authorizing the operation of the system based on the risk determination
- ▶ **Monitor:** Continuously monitoring and assessing the security controls for effectiveness

Who's affected

Federal agencies, state agencies that administer federal programs, entities funded by certain federal grants, and government contractors who exchange data directly with federal government systems.

Resources

- ▶ [TechTarget: Federal Information Security Act](#)
- ▶ [NIST: FISMA Implementation Project](#)

HEALTHCARE

The healthcare sector is one of the most regulated of all industries in terms of data protection. Healthcare providers and their business associates must comply with the Healthcare Insurance Portability and Accountability Act, which protects the privacy of patient data. Noncompliance can result in fines totalling millions of dollars.

HEALTHCARE INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

Summary

The Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA), which applies to healthcare providers, has requirements for protected health information (PHI) that is created, collected, maintained, and transmitted. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 extended the HIPAA requirements to business associates. The Office of Civil Rights within the U.S. Department of Health and Human services enforces HIPAA compliance and levies steep fines against providers as well as business associates for violating HIPAA provisions.

Key requirements

To protect electronic PHI (ePHI), HIPAA's Security Rule requires covered entities to maintain reasonable administrative, technical, and physical safeguards. The regulation doesn't prescribe specific practices, and each organization must determine what is considered "reasonable" based on its unique circumstances.

The rule has four core requirements:

- ▶ Ensuring the confidentiality, integrity, and availability of all ePHI that organizations create, receive, maintain, or transmit
- ▶ Identifying and protecting against "reasonably anticipated" threats to the security or integrity of the information
- ▶ Protecting against unauthorized use and disclosure
- ▶ Ensuring workforce compliance with the requirements

Who's affected

Covered entities include healthcare providers that transmit electronic data, as well as health plans and health clearinghouses. Additionally, business associates that carry out activities and functions on behalf of covered entities must comply with the same requirements.

Resources

- ▶ [Arctic Wolf: Simplify HIPAA Compliance](#)
- ▶ [HHS: Summary of the HIPAA Privacy Rule](#)
- ▶ [HHS: HIPAA Security Rule](#)



HEALTHCARE

HEALTHCARE INFORMATION TRUST ALLIANCE COMMON SECURITY FRAMEWORK

Summary

The Healthcare Information Trust Alliance (HITRUST) developed the Common Security Framework (CSF) based on a variety of federal and state regulations, frameworks, and standards. The CSF provides regulated healthcare organizations with a common set of standards they can adopt as well as use for evaluating their vendors.

Key requirements

The HITRUST CSF uses a risk-based approach that includes:

- ▶ Organizational factors such as geographic scope and business volume
- ▶ Regulatory factors that are based on compliance requirements specific to the organization's circumstances, including sector and geography
- ▶ System factors that impact data management risks, such as data storage and transmission, internet access, third-party access, number of users, and number of daily transactions

The framework also has allowances for alternate management, technical, or operational controls that can be applied under specific conditions

Resources

- ▶ [RSI Security: HITRUST Compliance: What You Need to Know](#)
- ▶ [HITRUST Alliance: Understanding and Leveraging the CSF](#)

LOCATION-SPECIFIC

States have enacted their own laws protecting the security and privacy of consumer data. If you do business in those states, you'll need to comply. Some laws are specific to industries, such as financial, while others apply across the board. Additionally, if you serve customers in the European Union, you need to comply with the General Data Protection Rule, regardless of where you're headquartered.

CALIFORNIA CONSUMER PRIVACY ACT

Summary

The California Consumer Privacy Act (CCPA), effective Jan. 1, 2020, is the first of its kind consumer privacy legislation in the United States. It gives consumers the ability to request, free of charge, information about what businesses collect about them. This includes what sources are collecting information, and for what purpose. They can also request to opt out from having their data sold, and/or request that their data be deleted. The California Attorney General enforces the law, which includes provisions for civil litigation and penalties.

Key requirements

The CCPA applies to any business that sells products and services to Californians—and even displaying a website could count as advertising in the state. The law, however, exempts entities that have \$25 million or less in revenues, collect data on fewer than 50,000 consumers, and derive less than half of their revenues from selling consumer data. The list of what personal data must be disclosed or deleted upon request is comprehensive and includes web browsing history, biometrics, and geolocation.

Who's affected

All for-profit businesses, regardless of their physical location, that fall under at least one of these three categories:

- ▶ Sell to California consumers and earn more than \$25 million in annual gross revenues
- ▶ Collect (buy, receive, access) data on more than 50,000 consumers
- ▶ Earn more than half of their revenues from selling personal data of consumers

Resources

- ▶ [Arctic Wolf: How the California Consumer Privacy Act Increases Your Cybersecurity Responsibilities](#)
- ▶ [American Bar Association: California Consumer Privacy Act](#)
- ▶ [Fortune: Here Comes America's First Privacy Law: What the CCPA Means for Businesses and Consumers](#)

LOCATION-SPECIFIC

NEW YORK SHIELD ACT

Summary

New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act, effective March 21, 2020, implements cybersecurity requirements for businesses that collect private data on state residents. The statute expands existing legislation, including the definition of private data. The law is not limited to consumer information, so employers and others also need to comply—or risk penalties.

Key requirements

The SHIELD Act has three main elements:

- ▶ Administrative safeguards, such as assessment of internal and external risks, while providing employee training
- ▶ Technical safeguards, such as assessment of security risks to networks, software design, and information processing
- ▶ Physical safeguards, such as protecting against unauthorized physical access and use during or after the collection, transportation, and disposal of data

Who's affected

Any entity or individual, regardless of physical location, who owns or licenses private digital data of New York state residents.

Resources

- ▶ [Arctic Wolf: New York State's Upcoming SHIELD Law: Is Your Business Ready?](#)
- ▶ [The National Law Review: New York Enacts the SHIELD Act](#)
- ▶ [Society for Human Resource Management: The New York Shield Act: What Employers Need to Know](#)

LOCATION-SPECIFIC

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES CYBERSECURITY REGULATION

Summary

The New York State Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 500) applies to financial institutions—including banks, mortgage and other lenders, and insurance companies—that are licensed, registered, or chartered under NYDFS. It imposes strict cybersecurity requirements that align with the NIST Cybersecurity Framework.

Key requirements

The regulation establishes minimum standards for protecting customer information and IT systems. Requirements include:

- ▶ Maintaining a cybersecurity program based on risk assessment for both internal and external risks, including the performance of annual penetration testing and bi-annual vulnerability assessments
- ▶ Implementing policies and procedures for identifying and responding to cybersecurity incidents
- ▶ Maintaining a program for assessing and mitigating IT systems' vulnerabilities
- ▶ Limiting user access privileges to sensitive data
- ▶ Developing a cybersecurity policy and incident response plan, as well as security policies for third-party service providers

Who's affected

A covered entity is defined by a person who operates under, or is required to operate under, a license, charter, registration, certificate, permit, accreditation, or other form of authorization under the State of New York Banking Law, Insurance Law, or Financial Services Law.

Resources

- ▶ [Arctic Wolf: Simplify Compliance for NY DFS Cybersecurity Requirements](#)
- ▶ [NYDFS: 23 NYCRR 500](#)

LOCATION-SPECIFIC

GENERAL DATA PROTECTION RULE

Summary

The General Data Protection Rule (GDPR), established by the European Commission, regulates data protection for entities that store or process personal data of EU citizens. In addition to protecting personal data, the rule gives consumers broad rights regarding their information, and imposes steep penalties for noncompliance. You don't need to have a business presence in the European Union to be subject to GDPR.

Key requirements

Some of the most important GDPR requirements include:

- ▶ Appointing a data protection officer
- ▶ Using a “privacy by design” approach
- ▶ Implementing data security measures
- ▶ Notifying regulators of data breaches within 72 hours

GDPR also gives consumers the right to access their data, be informed about data that's being collected, restrict processing of their data, and more.

Who's affected

All entities, regardless of their physical location, that collect and process data of European Union subjects and have more than 250 employees. Organizations with 250 or fewer employees also must comply if they process data systematically, which could include anything from sending out newsletters or using Google analytics to analyze website traffic, to storing employment data.

Resources

- ▶ [Arctic Wolf: Preparing for the Global Impact of GDPR](#)
- ▶ [CSO Online: GDPR: What You Need to Know to Stay Compliant](#)

LOCATION-SPECIFIC

OTHER STATE PRIVACY AND CYBERSECURITY LAWS

Summary

In addition to California and New York, all other states have their own laws protecting consumer privacy. In many cases they relate to disclosure of data breaches that impact personal data, and some states go so far as publishing a public database of these disclosures. Many states enact additional laws every year, expanding the protections.

States with comprehensive legislation include

- ▶ Delaware: Has protections for children, e-book users, library cardholders, and employees, while requiring a prominently posted privacy policy. In addition, the Delaware Data Insurance Data Security Act of 2019 requires insurance companies licensed to do business in the state to implement information security programs.
- ▶ Illinois: Protects biometric data, such as fingerprints and requires organizations to implement reasonable security measures against private data disclosure, unauthorized use, and modification.

Resources

- ▶ [Small Business Trends: What Does Your State's Law Require of Your Business Following a Data Breach?](#)
- ▶ [National Conference of State Legislatures: Consumer Data Privacy Legislation](#)
- ▶ [CompariTech: Which US States Best Protect Privacy Online?](#)

NEXT STEPS

Compliance is no longer a matter limited to highly regulated businesses.

Regardless of your industry, company size, or location, you need to comply with a variety of cybersecurity and privacy laws. Otherwise, you're putting yourself at risk for legal troubles, as well as potentially damaging your bottom line.

Do you have the tools you need to meet your industry, state, and federal regulation requirements?

The experts at Arctic Wolf®, the market leader in security operations, can help.

Gain protection and start experiencing industry-leading security operations as a concierge service. [Contact us](#) to find out how to better manage your risks and stay compliant in an evolving landscape.



CONTACT US

arcticwolf.com | 1.888.272.8429 | ask@arcticwolf.com
111 West Evelyn Avenue, Suite 115 | Sunnyvale, CA 94086

PERSONAL | PREDICTABLE | PROTECTION

