



TESSIAN

# CEO's Guide to Data Protection and Compliance

GDPR | CCPA | HIPAA | GLBA | PCI DSS

By 2024, CEOs will be held personally liable for data breaches. That's why it's essential the C-Suite understands the importance of privacy, data protection – and therefore cybersecurity – and how these functions support business goals.



Share this report





# Why cybersecurity and compliance matter now

Over the last several years – thanks largely to data privacy regulations – cybersecurity has become *less* siloed and *more* integrated with overall business functions. But in many organizations, security leaders still don’t have a seat at the table.

This disconnect with the board can make [communicating risk, opportunity, and cybersecurity ROI](#) pretty difficult and means compliance can be seen as more of a “box ticking exercise” than anything that actually supports the business.




But cybersecurity is more than a means to an end and remaining compliant is about more than avoiding fines. A **data-first (and therefore *human* first) security approach** can be a business enabler and competitive differentiator.

And in a few years, it could also keep CEOs out of jail.

By 2024 – [according to Gartner](#) – CEOs will be held personally liable for data breaches if it is found that the incidents occurred because the organization did not focus on cybersecurity or invest sufficiently in it.

The bottom line: Cybersecurity is mission critical. That means business leaders need to prioritize data protection and privacy. Step one is understanding the regulatory landscape.

## READERS WILL LEARN

-  How compliance standards like the GDPR, CCPA, HIPAA, GLBA, and PCI DSS have changed how businesses operate.
-  The benefits of ensuring compliance (beyond just avoiding fines) and why the C-suite should care.
-  The most effective ways to prevent data loss and satisfy compliance standards.



“To be successful in implementing security change, you have to bring the larger organization along on the journey. How do you get them to believe in the mission? How do you communicate the criticality? How do you win the hearts and minds of the people? CISOs no longer live in the back office and address just tech aspects. It’s about being a leader and using security to drive value.”



**KEVIN STORLI**  
Global CTO and UK CISO at PwC

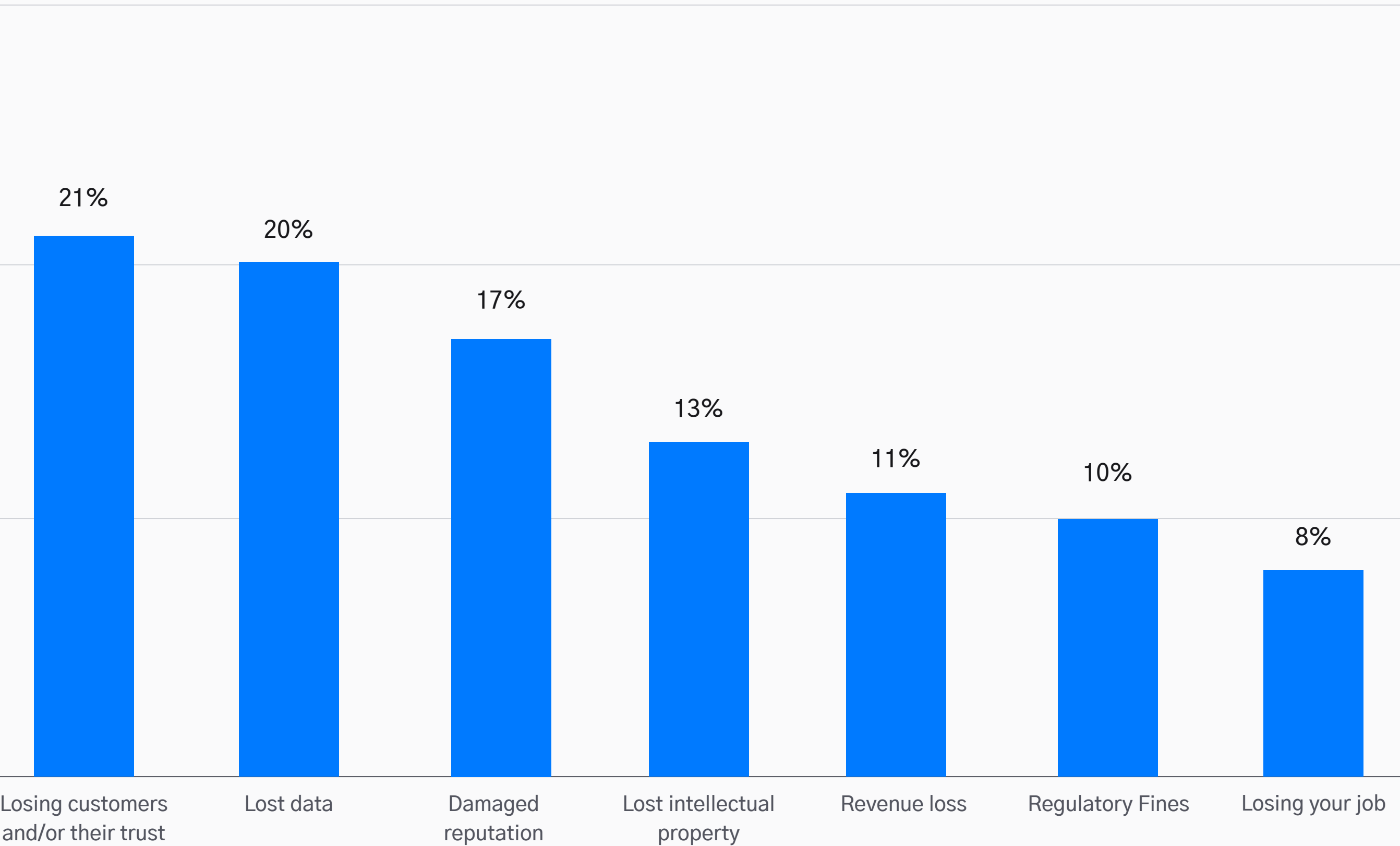
# Good privacy is good for business: how privacy creates value

We asked security leaders what they viewed as the biggest consequence of a data breach. Nearly [a quarter said losing customer trust](#). Just 10% said regulatory fines. Why does this matter?

It proves that compliance standards like GDPR, CCPA, HIPAA, GLBA, and PCI DSS have fundamentally changed how businesses across regions and industries operate. **Customers, clients, and employees don't just care about privacy. They expect it.**

While this means a breach is bad news for everyone involved – employees, the larger organization, and third parties like customers, suppliers, or patients – it *also* means there are benefits of privacy well beyond simply avoiding multi-million dollar penalties.

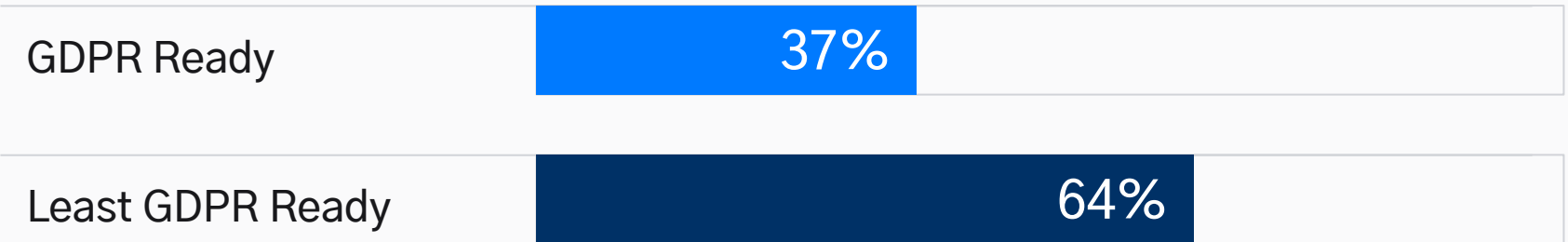
In your opinion, what is the biggest consequence of a data breach to an organization?



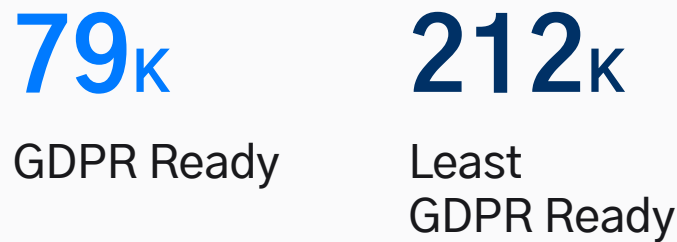
Percentage who had a data breach



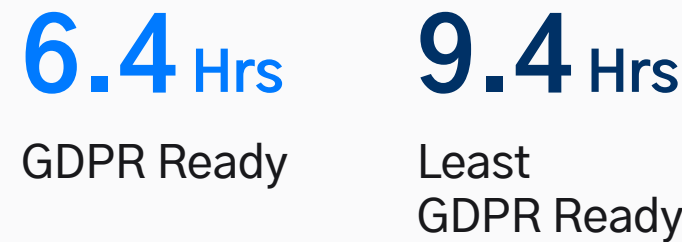
Percentage who had breach losses > \$500,000



Number of records impacted



System downtime



According to [Cisco’s global survey](#) of security professionals and business leaders, **97% of organizations who meet most (or all) the GDPR requirements enjoy one or more of the following benefits:**

1. COMPETITIVE ADVANTAGE

Whether or not your business operates in a highly-regulated industry or region (skip to pages 6, 7, and 8 for a high-level overview of 25 different laws and standards), **a strong privacy program and a track record of transparency are competitive differentiators.** Yes, protecting data could help you attract new customers and clients *and* help you keep the ones you already have. Bonus: Only [28% of companies](#) are currently fully compliant with the GDPR, the “gold standard” of compliance. That translates to massive opportunity for those who put data privacy and protection first.

2. INVESTOR APPEAL

Given the number of high-profile data breaches we’ve seen in recent years (and the far-reaching consequences of a data breach) investors are naturally more interested in privacy-mature organizations.

3. BREACH MITIGATION

Organizations that fulfill their data privacy obligations have fewer and less costly breaches. According to one study, GDPR-ready companies saw fewer records impacted, suffered smaller losses, and had shorter system downtime than the least GDPR-ready companies.

4. RICH DATA INSIGHTS

Businesses typically undergo a “data mapping” or “data discovery” phase as a part of their compliance and data loss prevention program. Oftentimes, in doing so, they uncover rich insights into customer behavior and internal processes. That means **privacy and compliance can actually help drive innovation, improve marketing efforts, and increase operational efficiency.**



“You’re only going to win more work if you’re reputable. And you’re only going to be reputable if you demonstrate you have a strong information security framework.”

 **MARK PARR**  
Global Director, HFW

While we take a deeper dive into data requirements under the GDPR, CCPA, HIPAA, GLBA, and PCI DSS starting on **page 9** and detail the breach notification process on **page 19**, you can use this checklist as a guide to help you understand what steps you need to take to ensure general compliance.

- ✓ Data Discovery
- ✓ Implementation of Security Controls
- ✓ Consent Management
- ✓ Data Minimization
- ✓ Usage Monitoring
- ✓ Breach Notification

For more information about each of these steps – including a checklist – [download Tessian’s Compliance Toolkit.](#)



# 6 Steps to Data Protection & Compliance

While every piece of data protection legislation has different requirements, you can use this checklist as a catch-all for broadly ensuring compliance.





## Data Discovery

Before you can protect your assets, you have to know what you have. Identify all of your organization’s applications, devices, servers, and people. From there prioritize. Some data is more sensitive than others, some vectors are more vulnerable than others, and you’ll need consent to even process some types of data.



### TOP TIP

When prioritizing, you should review business objectives, learn what systems and processes different teams and departments use, and understand your organization’s risk appetite. That way, they’re aligned with the goals of the organization and have a better understanding of how people work with (or around) cybersecurity.



### TOP TIP

It’s essential that the controls you implement don’t make it harder (or impossible) for your employees to get their jobs done. Likewise, security should be light on admins.



## Implementation of Security Controls

After you know what you have – and what’s most important to protect – you can start exploring tools, policies, and procedures that will help you build an effective data loss prevention program. This will include network, application, cloud, email, and physical security.



Download Compliance Toolkit Now →

# Data privacy regulation across the globe

**1 CANADA** — [Personal Information Protection and Electronic Documents Act \(PIPEDA\)](#)

A comprehensive privacy law that applies to all private sector organizations (unless covered by provincial privacy law).

**2 UNITED STATES (CALIFORNIA)** — [California Consumer Privacy Act \(CCPA\)](#)

Covers big businesses and businesses that “sell” personal information (this could include you, even if you don’t realize it! Skip to page 11 to learn more.)

**3 UNITED STATES (NEW YORK)** — [New York SHIELD Act](#)

Data breach notification law that ALSO requires businesses to implement a data security program.

**4 BRAZIL** — [Brazilian General Data Protection Law \(LGPD\)](#)

Known as “Brazil’s GDPR,” the LGPD imposes data processing principles on all organizations and provides consumers with legal rights.

**5 ARGENTINA** — [Personal Data Protection Act](#)

A comprehensive privacy law that applies to all people and organizations doing business in Argentina.

**6 EUROPEAN UNION** — [General Data Protection Act \(GDPR\)](#)

The world’s “gold standard” data protection law, covering all aspects of personal information processing and privacy rights.

**7 UNITED KINGDOM** — [Data Protection Act](#)

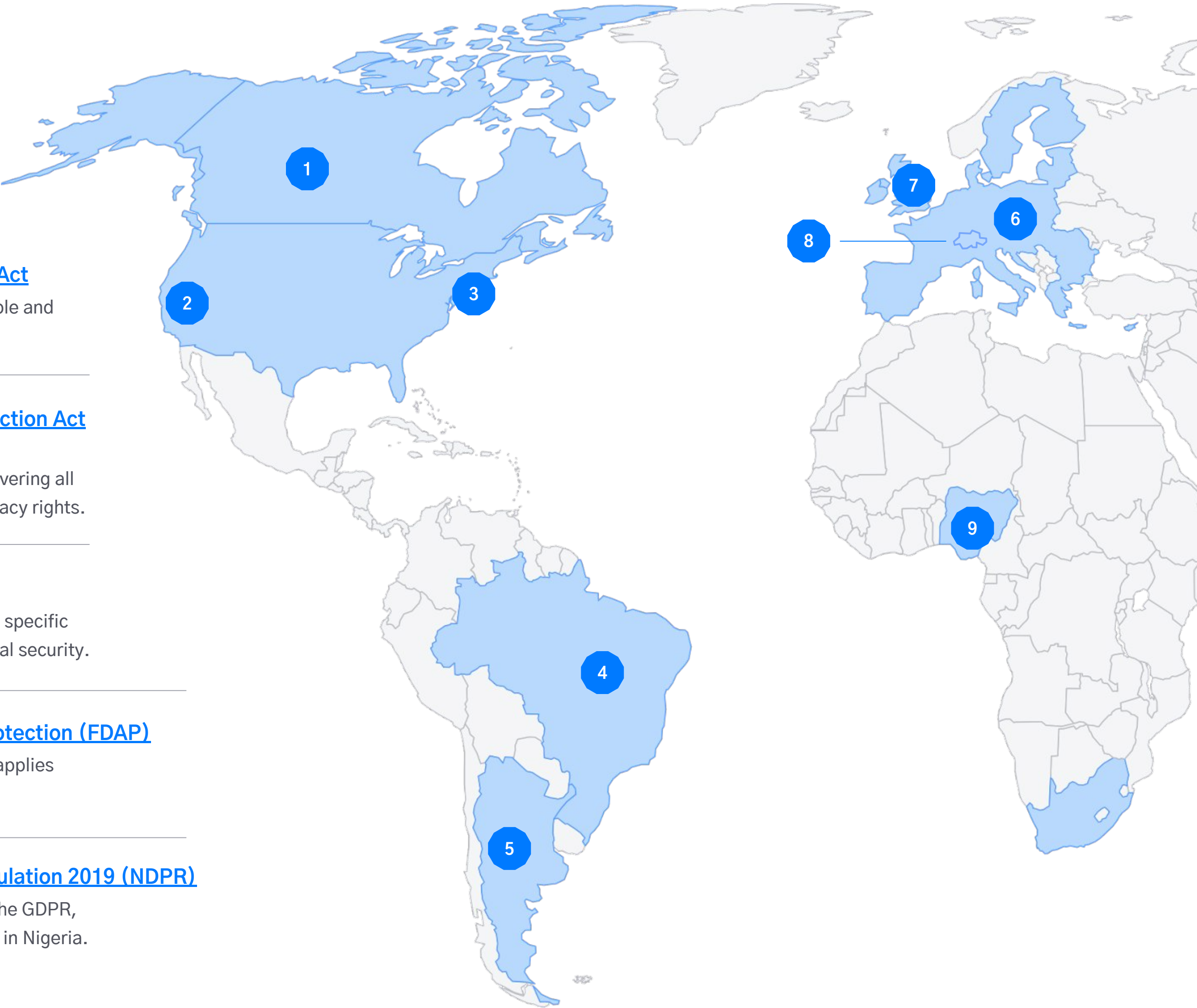
Implements the EU GDPR in the UK, providing some specific exemptions in areas such as immigration and national security.

**8 SWITZERLAND** — [Federal Act on Data Protection \(FDAP\)](#)

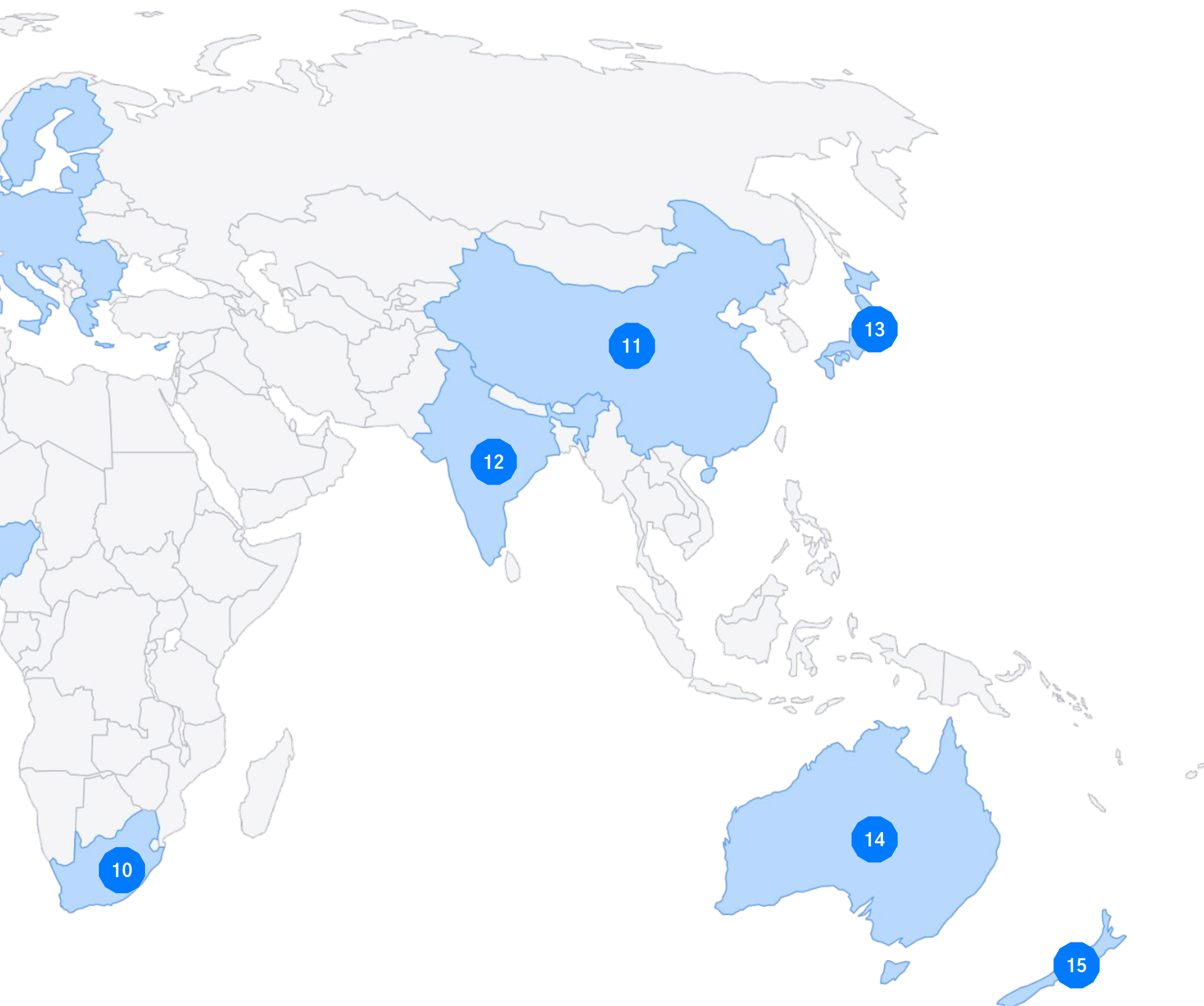
Like the GDPR, but with smaller fines — and it also applies to “legal persons” (e.g. corporations).

**9 NIGERIA** — [Nigerian Data Protection Regulation 2019 \(NDPR\)](#)

A strict data protection law with similar wording to the GDPR, applying to anyone processing personal information in Nigeria.







**10 SOUTH AFRICA — [Protection of Personal Information Act \(POPIA\)](#)**

Another broad, GDPR-inspired privacy law affecting all organizations operating in South Africa.

**12 INDIA — [Personal Data Protection Bill](#)**

A strict and sweeping data protection law working its way through India’s lawmaking bodies — due to pass in 2020.

**14 AUSTRALIA — [Privacy Act 1988](#)**

Imposes the 13 Australian Privacy Principles, such as transparency and security, on public bodies and businesses with a turnover of over AUD 3 million.

**11 CHINA — [Personal Information Security Specification](#)**

One of several laws covering privacy and information security in China — aimed at businesses.

**13 JAPAN — [Act on the Protection of Personal Information \(APPI\)](#)**

Applies to all private sector organizations and requires consent for the sharing of personal information.

**15 NEW ZEALAND — [Privacy Act 2020](#)**

Comes into effect on December 1, 2020, with new data breach notification rules, bigger fines, and application to foreign businesses.

“Cybersecurity professionals have this absolute obligation to maintain security and respond to threats appropriately, all whilst respecting privacy rights and obligations. That’s a challenge.”



**EMILY FISHER**  
Data Privacy Manager, Clifford Chance

# Data privacy by industry



## App developers

[Payment Card Industry Mobile Payment Acceptance Security Guidelines →](#)

Provides standards for accepting payments over mobile apps.



## Children's online services

[Children's Online Privacy Protection Act \(COPPA\) →](#)

US federal law applying to anyone operating a commercial website, online service, or mobile app aimed at children under 13.



## Cloud service providers

[ISO/IEC 27017:2015 →](#)

Code of practice providing information security standards from cloud service providers.



## Energy

[ISO/IEC TR 27019 →](#)

Information security guidelines for utilities providers.



## Finance

[Gramm–Leach–Bliley Act \(GLBA\) →](#)

US federal law for any business that is “significantly engaged in providing financial products or services.”

## Retail/eCommerce/ Payment processing

[Payment Card Industry Data Security Standard \(PCI DSS\) →](#)

Applies to all organizations that accept, transmit, or store information associated with payment cards.



## Healthcare

[Health Insurance Portability and Accountability Act \(HIPAA\) →](#)

Covers healthcare providers, health plans, health clearinghouses, and their business associates.



## Legal/Forensics

[ISO/IEC 27037:2012 →](#)

Guidelines for identification, collection, acquisition, and preservation of digital evidence.



## Manufacturers

[Payment Card Industry PIN Transaction Security \(PCI PTS\) →](#)

Helps manufacturers create secure payment-processing equipment.



## Software developers

[Payment Application Data Security Standard \(PA-DSS\) →](#)

Helps developers create secure payment apps.





# GDPR

## Overview

### What is it?

The world’s “gold standard” for data protection laws that covers all aspects of personal information processing and privacy rights

### Who enforces it?

The Data Protection Authorities that operate in each country where the GDPR applies. In the UK, it’s the Information Commissioner’s Office (ICO)

### When was it enacted?

May 25, 2018

### Who is obligated to comply?

Any organization or person that collects personal data or behavioral information from someone in the EU

### What are the penalties for non-compliance?

A fine up to €20 million or 4% of a company’s annual revenue, whichever is higher

“Tessian exceeded the expectations of our GDPR team. You simply cannot beat seeing for yourself what the product is capable of against your own organization’s data.”



**MARK ELIAS**  
IT Infrastructure Manager, Coastal Housing

### What data is protected



- Personal data (information that relates to an identifiable individual) including:
  - Name
  - Address
  - ID card/passport number
  - Credit card information
  - Cultural profile
  - IP address
  - Health information

### Special categories of data



- Racial or ethnic origin
- Sexual orientation
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Genetic, biometric, of health data
- Data related to criminal convictions or offenses (not “special category data,” but also requires special protection)

### What are the requirements under GDPR?

- Organizations must only process personal data where they have a lawful basis for doing so. For example: they have the consent of the individual, they are legally obliged to process the individual’s personal data, and/or it is in their legitimate interests to process the individual’s personal data.
- Organizations must facilitate the data subject’s rights, including the rights of access, erasure, rectification, and data portability
- Data can (normally) only be processed for the reasons it was collected
- Data must be accurate and kept up-to-date or should be erased
- Data must be stored no longer than necessary (specifically when a subject is identifiable)
- Data must be processed and stored securely and should be pseudonymized, encrypted, or anonymized where appropriate
- Anyone who handles data (full-time staff, third-party contractors, temporary employees, volunteers) should be trained in data protection, privacy, and handling
- In most cases, organizations must appoint a Data Protection Officer (DPO)
- Organizations must take appropriate technical and organizational measures to ensure the level of security is appropriate to risk
- Data protection authorities (and affected data subjects) must be notified in the event of a data breach



# GDPR

## Biggest Breaches (and Fines) to Date

### OTHER RESOURCES

[GDPR Enforcement Tracker →](#)  
[10 Biggest GDPR Fines of 2020 \(So Far\) →](#)  
[3 Ways GDPR Has Affected Cybersecurity →](#)

\$124  
million\*



### What happened

383 million guest records (30 million EU residents) were exposed after the hotel chain's guest reservation database was compromised. PI like guests' names, addresses, passport numbers, and payment card information was exposed. Note: The hack originated in Starwood Group's reservation system in 2014. While Marriott acquired Starwood in 2016, the hack wasn't detected until September 2018.

### How it could have been avoided

The ICO found that Marriott failed to perform adequate due diligence after acquiring Starwood. They should have done more to safeguard their systems with a stronger [data loss prevention \(DLP\) strategy](#) and utilized de-identification methods.

\* Amount proposed by the ICO in July 2019. The fine hasn't yet been finalized.

\$56.6  
million



### What happened

In early 2019, french regulator CNIL found that Google wasn't sufficiently informing customers about how they collected data to personalize advertising. That means that there wasn't *actually* a data breach. Instead, Google was fined for a lack of transparency.

### How it could have been avoided

To start, Google shouldn't have "pre-ticked" the option to personalize ads for new users creating an account. Google also should have provided more information to users in consent policies, *and* should have granted users more control over how their personal data was processed.

\$56.6  
million



### What happened

H&M's GDPR violations involved the "monitoring of several hundred employees." After employees took vacation or sick leave, they were required to attend a return-to-work meeting. Some of these meetings were recorded and accessible to over 50 H&M managers who gained "a broad knowledge of their employees' private lives" which was *then* used to help evaluate employees' performance and make decisions about their employment.

### How it could have been avoided

H&M shouldn't have collected – or shared – personal information, particularly special categories of data about people's health and beliefs **without doing so for a specific and justifiable purpose**. H&M should also have placed strict access controls on the data and the company should not have used this data to make decisions about people's employment.







# CCPA

## Overview

### What is it?

Covers big businesses and businesses that “sell” personal information (this could include you, even if you don’t realize it!)

### Who enforces it?

The California Attorney General

### When was it enacted?

January 1, 2020

### Who is obligated to comply?

If you have a website that attracts visitors from around the world, chances are you’re obligated to satisfy the CCPA. It applies to any for-profit business in the world that has an annual gross revenue in excess of \$25 million, that buys, sells, or shares the personal information of more than 50,000 California residents annually, or that earns 50% or more of its annual revenues from selling consumers’ PI.

### What are the penalties for non-compliance?

Civil penalties can amount to \$7,500 per violation. Statutory damages related to breaches range from \$100 to \$750 per consumer, per incident or actual damages, whichever is greater.

## What data is protected



- Personal data (information that relates to an identifiable individual) including:
  - Name
  - Address
  - ID card/social security number
  - Credit card information
  - Cultural profile
  - IP address
  - Medical information
  - Biometric data
  - Health insurance information
- The CCPA’s definition of “personal data” is even broader than the GDPR’s and includes:
  - [IP address](#)
  - [Cookie data](#)
  - [Device ID](#)
  - [Geolocation data](#)
  - [Pixel tags](#)

## What are the requirements under CCPA?

- Organizations must uphold the CCPA Consumer Rights, including:
  - The right to know
  - The right to delete
  - The right to opt-out
  - The right to non-discrimination
  - The right to opt-in (for minors)
- Organizations must maintain reasonable security procedures and practices in order to prevent unauthorized access, exfiltration, theft, or disclosure
- Organizations must provide notice to consumers including:
  - Privacy policy
  - Notice of collection
  - Notice of the right to opt-out
  - Notice of financial incentives
- Organizations must not “sell” personal information to another business or third-party
- The California Attorney General (and affected data subjects) must be notified in the event of a data breach



# CCPA

## Biggest Breaches (and Fines) to Date

\$500 million to  
\$3.75 billion



### What happened

According to the [case docket](#) and [Zoom’s blog post](#), Zoom shared user data – including device type, advertising ID, mobile OS type, and more – with Facebook without notifying users. This appears to have been the result of Zoom allowing users to “Login with Facebook”, but even *non*-Facebook users were affected. So, how big was the breach? According to the complaint, “millions” of users could claim statutory damages.

### How it could have been avoided

While this may seem like an issue relating to opt-ins, it has more to do with cybersecurity. Because Zoom is alleged to have “failed to properly safeguard the personal information of users”, the potential violation will be classed as a failure to implement reasonable security.

Undisclosed  
amount



### What happened

According to the [case docket](#) and [Marriott’s own announcement](#), the PI of 5.2 million people was exposed in a data breach after the login credentials of two employees were compromised. Marriott believes the activity started in mid-January 2020. The login credentials weren’t disabled until the end of February.

### How it could have been avoided

Marriott is being accused of failing to “institute the most basic cybersecurity policies and procedures”, failing to “exercise reasonable care” *and* failing to train employees on policies and procedures. In a nutshell: Marriott could have avoided the breach with stronger cybersecurity controls (**network security** and [email security](#) specifically) and training.

### OTHER RESOURCES

[CIS’s Guide to CCPA’s Minimum Requirements](#) →

[CCPA FAQs: Your Guide to California’s New Privacy Law](#) →

[CCPA and GDPR Comparison Chart](#) →

\$1 million to  
\$7.5 million



### What happened

According to the [case docket](#) and [data breach notification](#), between September 16, 2019 and November 11, 2019, hackers deployed malware to the website of children’s retailer Hanna Andersson (hosted by Salesforce) and scraped customers’ names and payment information. The PI of over 10,000 California consumers was later found being sold on the Dark Web. The Office of the Attorney General and consumers weren’t notified until over a month later.

### How it could have been avoided

While Hanna Andersson and Salesforce should have better protected users’ PI with security controls *and* more effectively monitored the website and ecommerce platform for security vulnerabilities, they’re also being accused of failing to notify consumers of the breach properly. This shows the importance of investigation and remediation and seamless reporting processes.





# HIPAA

## Overview

### What is it?

Healthcare-specific federal law that protects sensitive patient health information

### Who enforces it?

The US Department of Health & Human Services, and other agencies such as Centers for Medicare and Medicaid

### When was it enacted?

August 21, 1996

### Who is obligated to comply?

Most health care providers (including doctors, clinics, hospitals, nursing homes, pharmacies), health plans, healthcare clearinghouses, and their business associates

### What are the penalties for non-compliance?

Fines of up to \$50,000 per violation, with an annual maximum of \$1.5 million per violation and/or prison terms of up to 10 years

## What data is protected



- Public Health Information (PHI) includes any information that could be used to identify an individual, such as:
  - Names
  - Dates directly related to an individual
  - Phone numbers
  - Email addresses
  - Social Security numbers
  - Medical records/medical record numbers
  - Health insurance information
  - Account numbers
  - Vehicle identifiers
  - Device identifiers and serial numbers
  - IP numbers
  - Biometric identifiers
  - Full photographic images
  - Geographical identifiers

“The added value of Tessian is that it influences behavior. That really resonated with the board and helped me make a strong business case. While I can’t show how cybersecurity creates revenue, I can show the potential fines we could avoid because of our investment in Tessian.”



CAS DE BIE  
CIO at Cordaan



## What are the requirements under HIPAA?

- Organizations must carry out a risk assessment
- Organizations must implement administrative, physical, and technical safeguards, including training to ensure compliance by their employees
- Organizations must ensure the confidentiality, integrity, and availability of electronic PHI (e-PHI) they create, receive, maintain, or transmit
- Organizations must identify and protect against reasonably anticipated threats to the security or integrity of e-PHI and protect against impermissible uses or disclosures
- Organizations must modify and review their security measures to continue protecting e-PHI in a changing environment (internal and external)
- Organizations must notify relevant parties (patients, the HHS, etc.) in the event of a data breach





# HIPAA

## Biggest Breaches (and Fines) to Date

OTHER RESOURCES

[At A Glance: Data Loss Prevention in Healthcare](#) →

[HIPAA Basics for Providers: Privacy, Security, and Breach Notification Rules](#) →

[US Data Privacy Laws: What You Need to Know](#) →

\$16 million



### What happened

After Anthem Blue Cross’ computer system was hacked, the data of around 78.8 million people was stolen, including names, birthdays, addresses, medical IDs, social security numbers, and employment information. The insurance company settled with affected patients for \$115 million in 2017 before shelling out \$16 million in the HIPAA settlement.

### How it could have been avoided

While Anthem denies liability, specialists say Anthem didn’t take steps to protect data in its computers through encryption and other controls, policies, and procedures that would prevent hackers from gaining access to employee login credentials and other systems and data. **Bonus: Did you know that credentials are the [most frequently compromised](#) “type” of data in phishing attacks?**

\$6.85 million



### What happened

In May 2014, Premera Blue Cross was targeted by a spear phishing attack which installed malware on the healthcare provider’s network, giving them access to their IT system. After going undetected for nine months, the PI of more than 10.4 million people was exposed, including health plans, clinical information, names, addresses, and social security numbers.

### How it could have been avoided

The OCR found “systemic non-compliance” with the HIPAA Rules which means Premera Blue Cross should have invested more money, time, and resources into privacy and cybersecurity, conducted an enterprise-wide risk analysis, and implemented risk management and audit controls. In particular, though, they should have invested more in [inbound email security](#) to prevent the spear phishing attack.

Undisclosed amount



### What happened

After multiple health insurers (including Anthem and Premera Blue Cross) were breached, Excellus *proactively* hired a cybersecurity firm to conduct a forensic assessment of its IT systems. They found that hackers had gained access to administrative controls and therefore data (financial account information, claims information, names, dates of birth, social security numbers, etc.) related to 10.5 million people. According to financial filings from 2015, the breach cost Excellus \$17.3 million in the 4.5 months following its discovery.

### How it could have been avoided

While it appears the HIPAA investigation is (still) ongoing – and they claim the data was encrypted – any pending violations will be related to a failure to protect sensitive data with administrative, physical, and technical controls.







# GLBA

## Overview

### What is it?

US federal law requiring financial institutions to explain how they use, share, and protect customers’ personal information

### Who enforces it?

Various agencies, including the Federal Trade Commission (FTC) and federal banking authorities, and state-level insurance regulators

### When was it enacted?

November 1999

### Who is obligated to comply?

Any business that is “significantly engaged in providing financial products or services,” including banks, securities firms, insurance companies, financial advisers, and other financial service providers

### What are the penalties for non-compliance?

Financial institutions can face fines of up to \$500,000, 5 years imprisonment, or both

### What data is protected



- Names
- Addresses
- Phone numbers
- Bank account numbers
- Credit card numbers
- Income and credit histories
- Social Security numbers

## EVERCORE

“We were looking for the right data loss prevention solution for two years. We loved the machine learning-powered approach Tessian offered.”



CHRIS TUREK  
CIO at Evercore

### What are the requirements under GLBA?

- Financial privacy rule:
  - Provide a privacy policy explaining how personal information is collected
  - Allow customers to opt out of the disclosure of their non-public personal information to non-affiliated third parties
- Pretexting rule:
  - Safeguard against the obtaining of financial information via false, fictitious, or fraudulent statements
- Safeguards rule:
  - Designate one or more employees to coordinate an information security program
  - Identify and assess risks to personal information in all operational areas
  - Evaluate the effectiveness of current safeguards
  - Design and implement a safeguards program
  - Only use service providers that can maintain appropriate safeguards
  - Implement a contract with service providers ensuring that they will maintain safeguards
  - Oversee service providers’ processing of personal information
  - Evaluate and adjust the safeguards program in light of relevant circumstances, operational changes, and the results of security testing





# GLBA

## Biggest Breaches (and Fines) to Date\*

### OTHER RESOURCES

[Ultimate Guide to Data Protection and Compliance in Financial Services](#) →

[How to Comply With the GLBA](#) →

[FDIC's Compliance Manual for GLBA](#) →

## \$575 million



### What happened

Between May and July 2017, hackers exploited a vulnerability in Equifax's unpatched software and gained access to the private records of over 147 million customers. In January 2020, the company agreed to a global settlement with the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau, and 50 U.S. States and Territories. The settlement *also* included a \$425 million payout to customers who were affected by the breach.

### How it could have been avoided

Equifax "failed to undertake numerous basic security measures" and, according to a House Oversight Committee report, the breach was "entirely preventable", had the credit agency patched a vulnerability they were warned about months prior.

## Undisclosed amount



### What happened

This one isn't a breach in the sense that customer data was exposed. It's simply a breach of the GLBA's Safeguards Rule. In a nationwide sweep monitoring compliance with federal privacy laws, Nationwide was found to have failed to comply with a number of data requirements (see below). In the end, the company was ordered to retain an independent professional to certify its security program on an ongoing basis. No fine was issued.

### How it could have been avoided

Again, it comes down to [DLP](#). Nationwide should have assessed risks to sensitive customer information, implemented safeguards to control these risks, trained employees on information security issues, maintained clearer oversight of how loan holders' handle customer information, and better monitored its computer network for vulnerabilities.

## Undisclosed amount



### What happened

In 2018, the FTC filed a complaint against PayPal – which acquired Venmo in 2014 – for failing to satisfy data requirements contained in both the GLBA and FTC Act *and* for misleading customers.

### How it could have been avoided

According to the FTC, Venmo didn't have a written information security program until August 2014 and, until 2015, hadn't implemented basic safeguards to protect data *or* created processes for customer support. **Step one? Data discovery.**





# PCI DSS

## Overview

### What is it?

Information security standard protecting credit card data

### Who enforces it?

Credit card companies that are members of the PCI Security Standards Council: American Express, Discover, JCB International, MasterCard and Visa Inc.

### When was it enacted?

December 2004

### Who is obligated to comply?

People and organizations working with and associated with payment cards, including: merchants, financial institutions, point-of-sale vendors, hardware and software developers

### What are the penalties for non-compliance?

While penalties are rarely made public (and vary depending on the contract between the credit card company and the card-issuing bank, and between the bank and the merchant or financial institution) organizations can be fined up to \$100,000 a month. See Resources on the next page for more information.

## What data is protected



### Cardholder data

- The full primary account number (PAN) (long card number)
- Full PAN in combination with:
  - Cardholder name
  - Expiry date
  - Service code (CVV2/security code)

## TESSIAN RESEARCH

### Cashing in: How hackers target retailers with phishing attacks

Phishing attacks for retailers, decision makers:

| Category          | Percentage |
|-------------------|------------|
| Phishing attacks  | 24%        |
| Malware           | 14%        |
| Denial of Service | 10%        |
| Insider threats   | 10%        |
| Other             | 10%        |

**Cashing in: How hackers target retailers with phishing attacks**

Cybercriminals will always follow the money. During peak shopping periods, retailers need to protect their people from a spike in phishing attacks.

**LEARN MORE →**

We see a similar trend around the busiest shopping period of the Black Friday.

In the US, shoppers spent a record \$13.9 billion on Black Friday in 2019, and a further \$1.1 billion on Cyber Monday. In the UK, Bankers' that transaction value was up 18.5% compared to Black Friday in 2018. 71 IT decision makers at UK and US retailers surveyed say the number of phishing receive rises during the Black Friday.

Furthermore, retailers say they need phishing attacks in the last three months - the so-called Golden Quarter - the rest of the year.

## What are the requirements under PCI DSS?

- Installing and maintaining a firewall
- Changing vendor-supplied default passwords and security parameters
- Protecting stored cardholder data via encryption, hashing, and other methods
- Encrypting cardholder data whenever transmitting over public networks
- Protecting systems against malware
- Developing and maintaining secure systems and applications
- Restricting access to cardholder data to authorized personnel on a “need to know” basis
- Identifying and authenticating access to networks, servers, and applications, including by assigning a unique ID to personnel
- Restricting physical access to cardholder data
- Logging and monitoring access to cardholder data and network resources
- Testing security systems and processes regularly
- Maintaining an information security policy, including staff training



# PCI DSS

## Biggest Breaches (and Fines\*) to Date

OTHER RESOURCES

[Payment Card Industry Standards: Compliance Burden or Opportunity](#) →

[Cashing In: How Hackers Target Retailers with Phishing Attacks](#) →

[PCI DSS Quick Reference Guide](#) →

### Undisclosed amount

### Heartland

#### What happened

While Heartland was actually deemed PCI DSS compliant at the time, they nonetheless suffered a breach after five men – who were involved in a worldwide hacking and data breach scheme – targeted them. 160 million customers had their credit card numbers stolen, resulting in hundreds of millions of dollars in losses. Heartland settled with Visa, Mastercard, and Amex, lost their PCI DSS compliance for 4 months, were forced to pay out/lost a total of \$200 million, and, within a few months, their stock price had fallen by over 77%.

#### How it could have been avoided

The payment processing provider was hacked by a successful SQL injection attack. So, how do you prevent one? Strong network security, strict access controls, and patch management.

### Undisclosed amount

### TJX

#### What happened

In 2007 – and over the course of 18 months – 94 million credit cards were compromised. Hackers allegedly planted unauthorized software on the retail giants computer network, enabling them to steal *hundreds* of files containing data on *millions* of accounts. Hackers also cracked TJX’s data encryption system, allowing them to access unencrypted data during the checkout/payment process.

#### How it could have been avoided

There were multiple points of attack in this breach, but better data encryption methods, firewalls, data monitoring, and training would all help safeguard TJX’s sensitive customer information.

### Undisclosed amount

### THE HOME DEPOT

#### What happened

Between April and September 2014, 56 million credit cards and 52 million email addresses were compromised after hackers accessed Home Depot’s network with a vendor’s username and password and installed malware on self-checkout registers.

#### How it could have been avoided

According to the SANS institute, “the implementation of P2P encryption and proper network segregation would have prevented the Home Depot data breach”. But, since credentials are frequently stolen in phishing and spear phishing attacks, strong [inbound email security](#) across the supply chain is also essential.

\*Because card companies don’t reveal any information about the fines that they have issued on acquiring banks and, likewise, banks don’t reveal any information about how they have recovered such fines from merchants, we can only provide information about the size of the breach and settlement costs, not the fines issued.





# What needs to happen immediately after a breach is discovered?

We talked about the long-term consequences of a breach, including cost, lost customer trust, and damaged reputation on page 3. But what about the *immediate aftermath*? The breach notification process is painful, labor-intensive, and generally involves several teams, including the C-suite.

On average, it takes companies [197 days to identify](#) and [69 days to contain a breach](#).

This list of to-dos should help you understand your regulatory obligations and what the minimum requirements are post-breach under compliance standards like the GDPR.



## Step 1: Investigation

- Assemble a team of experts and identify a data forensics team
- Consult with legal counsel
- Interview people who discovered the breach
- Follow internal reporting process
- Containment
  - Secure physical areas
  - Take systems offline
  - Remotely disable endpoints
  - Reset passwords
  - Change access rights
- Risk assessment:
  - Who was affected?
  - What data was compromised?
  - What caused the breach?
  - Who needs to know (including service providers who may have been affected)?
  - Do you need to hire external support?
  - How severe is the breach?

**The bottom line:** There’s a lot to do in the immediate aftermath of a breach and employees will have to drop tools on existing initiatives and revenue-generating projects. This will impact productivity and cause operational disruption. And that’s only step one.



## Step 2: Notification

Breaches generally have to be reported “as soon as possible”. In the case of GDPR, though, it’s within 72 hours. Within that period you must draft a notification letter explaining the nature of the breach, who has been affected, and what steps are being taken to mitigate the breach.

**Who has to be notified?** The enforcement agency (under the GDPR, it’s the lead Data Protection Authority), any individuals affected, and, under most US data breach laws, the state Attorney-General and consumer reporting agencies must also be notified.

Beyond just the mandatory notifications, most companies must also invest in crisis communications campaigns to control the narrative from a PR perspective and protect brand reputation. **These campaigns [cost an average of \\$400,000](#)** and involve strategic counsel from either external agencies or in-house PR teams who will prepare spokespeople for media interview sand press conferences, craft public statements, and field inbound media requests.

**Note:** Some US laws also require companies to offer paid credit monitoring services to individuals affected for a period of time following the breach. Organizing this can be very resource-intensive.



## Step 3: Evaluation

After a breach, companies need to show regulators that they are being proactive in trying to prevent further data loss. That means updating policies, implementing new solutions, training employees, and adopting a stronger security culture. **Fast.** This will also generally involve hiring new security professionals and onboarding external security/IT support. Don’t forget, you’ll need to report any changes to the regulators which requires even *more* time.

*You can avoid this arduous process and save valuable time and money by investing in cybersecurity solutions that prevent breaches from happening in the first place. It’s worth it. According to a recent report, the cost of non-compliance is [2.71 times higher than the cost of compliance](#).*

# How can Tessian help ensure compliance?



## General Data Protection Regulation (GDPR)

**INDUSTRY**  
All organizations that process personal data of EU residents.

**WHAT TYPE OF DATA**  
Personal data of EU residents.

**MANDATES**  
Protect against unauthorized or unlawful processing and accidental loss, destruction or damage of personal data.

**PENALTIES**  
Fines of up to 4% of the company’s annual worldwide turnover or €20 million, whichever is higher.

### HOW TESSIAN HELPS CUSTOMERS STAY COMPLIANT?

[Tessian Guardian](#) automatically prevents accidental sharing of personal data with unintended recipients.

[Tessian Enforcer](#) tracks and blocks personal data from being sent to unauthorized business accounts.



## California Consumer Privacy Act (CCPA)

**INDUSTRY**  
All businesses in California that meets at least one of the three criteria: Annual gross revenue of \$25 M; derive 50% of annual revenue from selling customer’s personal information; and buy / sell / receive / share personal information of >50,000 customers

**WHAT TYPE OF DATA**  
All end-user data collected by company websites using cookies and other tracking technology.

**MANDATES**  
Empower users with new data rights (the first in the US), such as the right to opt-out, the right to disclosure of what data has been collected, and the right to deletion of that data.

**PENALTIES**

- \$7,500 per intentional violation or \$750 per affected user
- \$2,500 for violations lacking intent

**HOW TESSIAN HELPS CUSTOMERS STAY COMPLIANT?**

[Tessian Guardian](#) automatically prevents accidental sharing of personal data with unintended recipients.

[Tessian Enforcer](#) tracks and blocks personal data from being sent to unauthorized business accounts.



## Health Insurance Portability & Accountability Act of 1996 (HIPAA)

**INDUSTRY**  
Healthcare

**WHAT TYPE OF DATA**  
Personally identifiable electronic health information (ePHI)

**MANDATES**

- Ensure the confidentiality, integrity and availability of all ePHI data through its lifecycle (created, received, maintained or transmitted)
- Identify and protect against threats and impermissible uses

**PENALTIES**

- Fines of up to \$50,000 per violation, with an annual maximum of \$1.5 million
- Prison terms of up to 10 years.

**HOW TESSIAN HELPS CUSTOMERS STAY COMPLIANT?**

[Tessian Guardian](#) prevents accidental data loss of sensitive patient data through misdirected emails.

[Tessian Enforcer](#) tracks and blocks confidential health information such as health insurance or social security numbers from being shared externally.



## Gramm–Leach–Bliley Act (GLBA)

**INDUSTRY**  
Organizations that provide financial products / services to customers.

**WHAT TYPE OF DATA**

- Nonpublic personal information (NPI)
- Personally identifiable information (PII)

**MANDATES**

- Ensure the secure collection, disclosure and protection of consumers’ NPI and PII
- Develop a written information security plan to protect customers’ NPI and PII

**PENALTIES**

- \$100,000 fine per violation for the organization
- \$10,000 fine per violation or up to 5 years in prison for personally liable officers

**HOW TESSIAN HELPS CUSTOMERS STAY COMPLIANT?**

Customers use [Tessian Constructor](#) to track and block PII such as social security and passport numbers from being sent externally.



## Payment Card Industry Data Security Standard (PCI DSS)

**INDUSTRY**  
Any industry that deals with cardholder data such as Retail, FSI.

**WHAT TYPE OF DATA**  
Payment card data in paper and electronic form during both storage and transmission.

**MANDATES**

- Implement strong access control programs around cardholder data.
- Maintain a comprehensive vulnerability program.

**PENALTIES**

- Non-compliance fines of up to \$100,000 / month
- Suspension of card acceptance

**HOW TESSIAN HELPS CUSTOMERS STAY COMPLIANT?**

Tessian can identify payment card data such as credit or debit card numbers and, if it appears it’s being sent to an incorrect or unauthorized recipient, it will be blocked.





Tessian is a leading cloud email security platform that intelligently protects organizations against advanced threats and data loss on email, while coaching people about security threats in-the-moment. Using machine learning and behavioral data science, Tessian automatically stops threats that evade legacy Secure Email Gateways, including advanced phishing attacks, business email compromise, accidental data loss and insider threats. Tessian’s intelligent approach not only strengthens email security but also builds smarter security cultures in the modern enterprise.

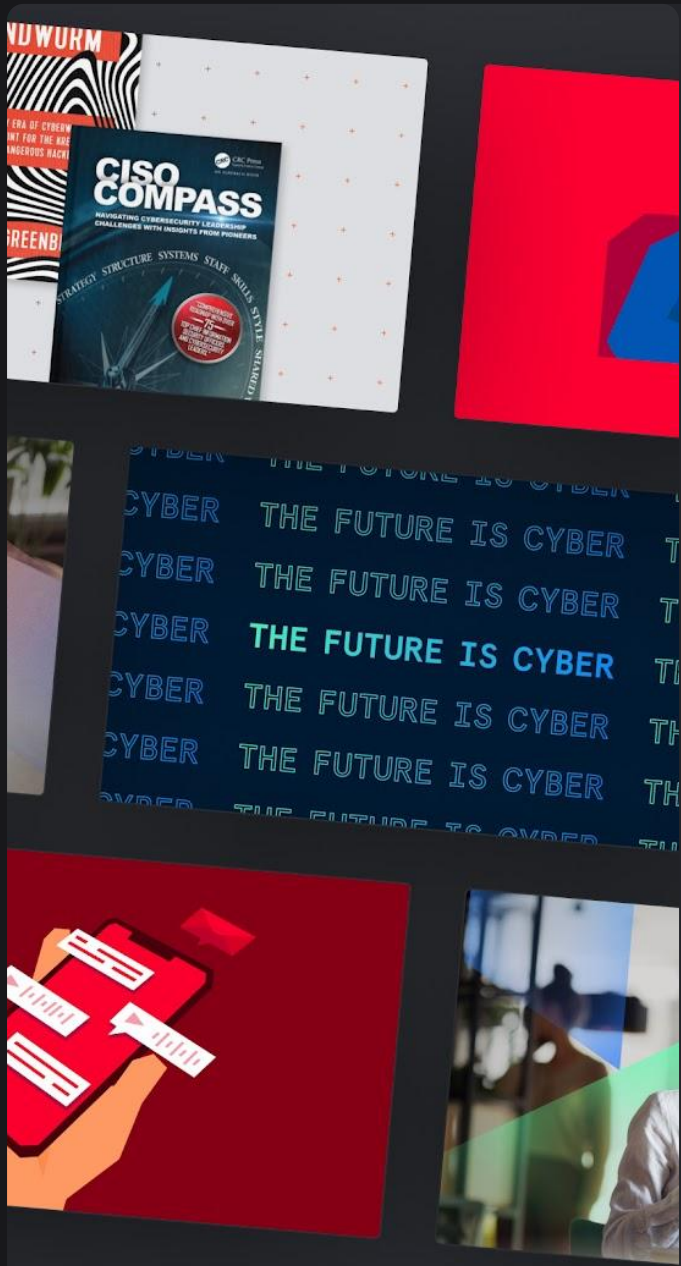
[TESSIAN.COM](https://tessian.com)



## Learn More About Tessian.

Want to learn more about how Tessian prevents spear phishing, business email compromise, account takeover, and other targeted email attacks?

[REQUEST A DEMO →](#)



## More Insights, Every Week.

Subscribe to the Tessian blog to get more insights straight to your inbox.

- Helpful resources and shareable guides
- Tips for CISOs
- Early access to our latest research and threat intelligence

[SIGN ME UP →](#)

Share this report



[TESSIAN.COM/RESEARCH →](https://tessian.com/research)