LUNAVI

# Why Are Data Compliance Standards Important?

Compliance standards equip businesses and their stakeholders to meet legal obligations and build commitment, trust, and responsibility when protecting personal data from theft, loss, or misuse.


**By 2023, 65% of the world's population will have its personal information covered under modern privacy regulations, up from 10% today.**

## THE CONSEQUENCES OF NONCOMPLIANCE

**By observing data compliance standards, organizations can maintain both their data security and customers' trust.**

After a breach, **80%** of consumers will defect from a business that has compromised their data

**52%** of consumers would pay the same for products or services from a different brand with better security

**Failing to adhere to regulations can result in significant financial loss:**

**GDPR fines** can reach as high as 4% of annual revenue or €20 million, whichever figure is higher.

**HIPAA fines** can reach $1.5 million per year.

The average cost of a **data breach** in 2021 was $4.24 million

# The Top Compliance Standards Compared

Organizations have different risks, threats, vulnerabilities, and risk tolerance. These frameworks provide guidance that should be customized to best suit their unique needs, rather than a one size fits all approach. As much as these frameworks vary, they have common aspects including:

**Transparency**
Alert customers that you are collecting their data and will only take what is necessary

**Monitoring**
Regularly take stock of potential vulnerabilities in your security system

**Integrity and security with customer data**
Utilize systems to backup and recover customer data, monitor, and control access

**Accountability**
Take on penalties (financial and legal), should data be breached

**Recovery Methods**
Having recovery methods and a plan of action in place, in case of a breach

## IMPLICATIONS AND FINES

**Do you know which standards apply to your organization?**
Don't leave it up to chance. Non-compliance can be costly – just look at these high-profile examples.

**$55 million**

**Google** (2019)
Improper disclosure to users on how data is collected, across Google's services, for personalized advertisements to users.

France's National Commission on Informatics and Liberty (CNIL) fined the company nearly $55 million. (Largest penalty to date by GDPR)

**$41.5 million**

**H&M** (2020)
Company managers kept excessive records on families, religions, and illnesses of their workforce through informal chats to be used during performance evaluations and employment decisions.

Fine in the amount of $41.5 million

**$33 million**

**TIM S.p.A.** (2020)
(Telecommunications Company) Violation of improper consent, excessive data retention, unlawful data processing, and data breaches. They commissioned call centers to make cold calls without proper consent.

Italian Data Protection Authority, Garante, issued a fine of $33 million

**$26 million**

**British Airways** (2019)
2018 data breach that leaked bank card numbers, expiration dates, and CVV codes due to poor security arrangements by the airline.

Information Commissioner's Office (ICO) fined the airline $26 million

| STANDARD | DESCRIPTION | AGENCIES AFFECTED |
|---|---|---|
| **NIST** (National Institute of Technology and Standards) | A set of optional standards, best practices, and recommendations for improving cybersecurity and risk management at the organizational level | Anyone who makes decisions about cybersecurity and cybersecurity risks in their organizations, and those responsible for implementing new IT policies |
| **CJIS** (Criminal Justice Information Services) | The division responsible for the collection, warehousing, and dissemination of relevant criminal justice information to the FBI and law enforcement, criminal justice, civilian, academic, employment, and licensing agencies | FBI, national crime information center (NCIC), Uniform crime reporting, (UCR), Integrated Automated Fingerprint Identification System (IAFIS), NCIC 200, National Incident-Based Reporting System (NIBRS), any local, state, or federal law enforcement agency |
| **HIPAA** (Health Insurance Portability & Accountability Act)/ HITECH Omnibus Rule | Manages the flow of healthcare information, stipulates how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and addresses some limitations on healthcare insurance coverage | Any person or organization that uses or creates protected health information on behalf of a covered entity while performing certain functions or activities |
| **PCI-DSS** (Payment Card Industry Data Security Standard) | An established information security standard which optimizes the security of credit, debit, and cash card transactions and protects cardholders against misuse of personal information | Applies to any organization involved in the processing, transmission, and storage of credit card information |
| **SOC 1 & 2** (AICPA-American Institute of Certified Public Accountants) | Documentation of the internal controls that are likely to be relevant to an audit of a customer's financial statements | Applies to any financial institution reporting on an examination of controls over its system relative to security, availability, processing integrity, confidentiality, or privacy |
| **GLB** (Gramm Leach Bliley) | Requirements of financial institutions to explain their Information-sharing practices to their customers and to safeguard sensitive data | Companies that offer consumers financial products or services like loans, financial or investment advice, or insurance |
| **SOX** (Sarbanes Oxley) | Annual audits that take place within public companies, within which they are bound by law to show evidence of accurate, secured financial reporting | Publicly traded companies and some private companies and government contractors |
| **CCGP** (Canadian Controlled Goods Program) | Controls the export of goods deemed to have military or national security significance under the Defense Production Act. (The definition of "goods" includes components and technology regardless of where they are manufactured.) | Organizations and individuals that are involved with controlled goods |
| **FedRAMP** (Federal Risk & Authorization Management Program) | Assessment and authorization process that federal government agencies have been directed to use to ensure security is in place when accessing Cloud computing products and services | Applies to Cloud Service Providers (CSPs) that sell to the Federal Government |
| **CCPA** (California Consumer Privacy Act) | A state statute intended to enhance privacy rights and consumer protection for residents of California, United States | Any organization doing business in California that collects the personal information of Californians |
| **GDPR** (General Data Protection Act) | A legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU) | Applies to any company or organization located in an EU State. It also applies to enterprises that offer goods and services or who monitor the behavior of any EU client or employee. (Any company that processes data of EU citizens, no matter where it is located, is subject to GDPR guidelines and penalties) |
| **ISO/IEC 27000 and 31000** (International Organization for Standardization) | A set of specifications for building an information security management system (ISMS). Designed to assist companies in managing cyber-attack risks and internal data security threats | Any organization using ISMS |

## Improve Your Security & Compliance Posture with Lunavi

Data compliance and information security can be complicated to manage in today's world of multi-cloud infrastructure, distributed workforces, and the ever-growing threat of hackers. Lunavi can help you navigate the numerous and complex regulations surrounding Data Compliance Standards and Security.

In addition to our annual audits for compliance standards like HIPAA and SOC 1 and 2, we can help you implement essential security operations and infrastructure from firewalls and endpoint management to fully managed Security Information and Event Management.

LEARN MORE

Contact us to get started today
or visit www.lunavi.com to learn more.

LUNAVI

## SOURCES


https://www.gartner.com/smarterwithgartner/gartner-predicts-for-the-future-of-privacy-2020)

https://www.varonis.com/blog/company-reputation-after-a-data-breach/

https://www.spirion.com/blog/gdpr-fines-increase/

https://www.immuta.com/articles/the-complete-guide-to-data-security-compliance-laws-and-regulations/#:~:text=The%20GDPR%20requires%20companies%20to,20%20million%2C%20whichever%20is%20higher

https://www.ibm.com/security/data-breach

https://www.tcdi.com/information-security-compliance-which-regulations/