FORTRA™

The Ultimate Guide to Data Protection

Everything you need to know about data protection but were afraid to ask

The 5 Key Questions of Data Protection

We live in a data-driven world. Some have dubbed data as the new oil. As the amount of data generated, mined, and stored grows at unprecedented rates, so increases the tolerance of leaving this data unprotected. Every security and privacy regulation, law, or standard includes requirements and best practices for data protection.

This simple guide attempts to answer five key questions about data protection:

What is data protection?
Why is it necessary?
When is it applicable?
Where is data protection applicable?
How can businesses protect their data?

What is Data Protection?

Data protection is safeguarding critical data from corruption, compromise, or loss and providing the capability to restore the data to a functional state should an incident render it inaccessible or unusable.

Data protection assures data integrity in transit and at rest, is available for authorized purposes, and complies with legal or regulatory requirements. Protected data should be available when needed and usable for its intended purpose.

Data protection strategies are evolving alongside two principles: data availability and data management. Data availability ensures that organizations or any other entity have the data they need to conduct business, even if the data is damaged or lost.

Data management is the process of storing, valuing, classifying, and protecting data assets from errors, malware, system vulnerabilities, physical outages, and disruptions.

Data Protection vs. Data Security vs. Data Privacy

Data protection is often used interchangeably with data security and data privacy. However, there are core differences between these terms, which are useful to define.

Data Privacy

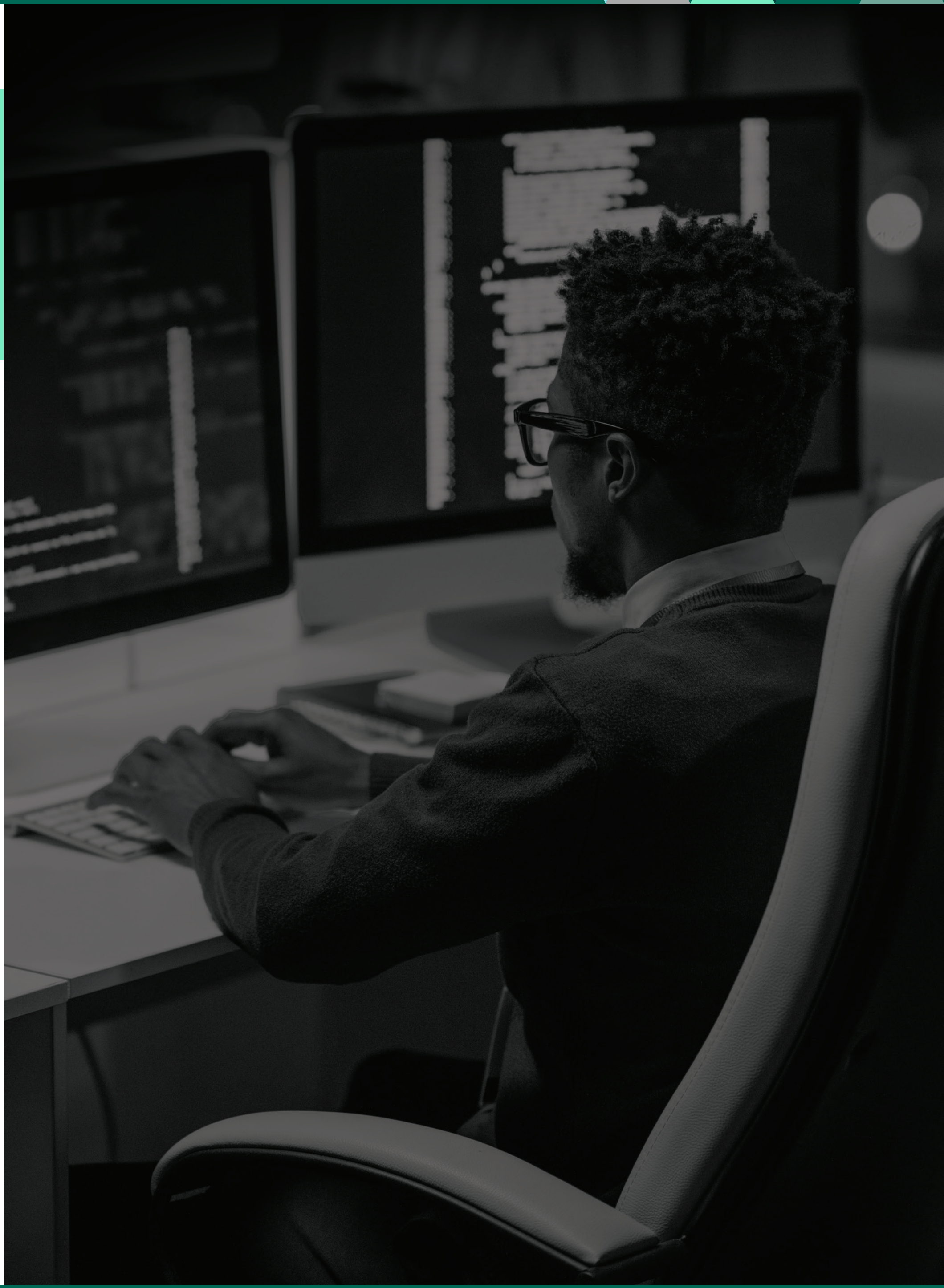
Data privacy refers to properly (and ethically) using and processing personal data by restoring control over data to the respective individuals. Simply put, data privacy enables individuals to decide and limit access to the use and sharing of their personal data. Citizens grant or remove control over their data privacy settings, determining which information is shared and with whom. Data privacy is governed by laws such as GDPR in the EU, PIPEDA in Canada, CCPA in California, and POPIA in South Africa to name a few.

Data Security

Data security protects digital data from theft, corruption, or unauthorized access throughout its entire lifecycle – from creation and storage to destruction. Data security involves everything from the physical security of the storage devices and hardware to administrative access controls and the security of software applications to organizational policies and procedures. Poor data security can harm data privacy.

Data Protection

Data protection covers data Confidentiality, Integrity, and Availability (the CIA triad of cybersecurity). It is a broader term that includes data security and data privacy. Data protection is the mechanism, tools, and procedures to enforce policy and regulation, and it is primarily an organization's responsibility.



History of Data Protection

Data Privacy Day is celebrated on January 28 each year on the anniversary of the signing of the Council of Europe's (CoE) Convention of Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Convention 108 represents the first legally binding international privacy and data protection treaty.

The following timeline depicts the history of the right to privacy and data protection from 1789 until May 25, 2018, highlighting the fundamental developments that laid the foundations of data protection and privacy as we know it today.

1789
US Bill of Rights

The Bill of Rights details the "right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures."

1890
The Right to Privacy

US Lawyers Samuel Warren and Louis Brandeis publish their groundbreaking article "The Right to Privacy," where privacy is defined as "the right to be let alone."

1948
UN Declaration of Human Rights

The United Nations Declaration of Human Rights, drafted by a committee chaired by Eleanor Roosevelt, enshrines the right to privacy. "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor attacks to his honor and reputation."

1950
European Convention on Human Rights

The European Convention on Human Rights provides protection for an individual's "private and family life, his home and his correspondence," subject to restrictions "in accordance with law" and "necessary in a democratic society."

1967
Freedom of Information Act

The Freedom of Information Act (FOIA) in the US gives citizens the right to request access to documents from state agencies.

1974
Privacy Act

The US Privacy Act established a code of fair information practice on the collection, maintenance, use and dissemination of personally identifiable information by federal agencies.

1980
OECD Guidelines on Data Protection

The first international effort to harmonize privacy and data protection, although not legally binding. Established the seven principles of notice, purpose, consent, security, disclosure, access and accountability.

1981
Convention 108

The Council of Europe adopts Convention 108 which renders the right to privacy a legal imperative. The Convention includes concepts that are reflected in modern data protection and privacy laws.

1995
European Data Protection Directive

The Data Protection Directive reflects technological advances and introduces new terms including processing, sensitive personal data, and consent.

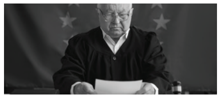
1996-1999
US HIPAA, COPPA, GLBA

The late 90s saw the introduction of sector specific privacy regulations that continue to shape the US privacy landscape: Health Insurance Portability and Accountability Act (HIPAA), Children's Online Privacy Protection Act (COPPA), and Gramm-Leach-Bliley Act (GLBA).

2002
EU ePrivacy Directive

The Directive on Privacy and Electronic Communications complements the Data Protection Directive and covers all issues of private electronic communication and governs cookies and tracking technology.

2014
The Right to be Forgotten



EU Court of Justice ruling finds that European law gives citizens the right to ask search engines like Google to remove results for queries that include their name.

2016
GDPR Approval

The EU Parliament approves the General Data Protection Regulation after 4 years of discussions.

May 25, 2018

GDPR is enforced replacing the Data Protection Act.

While much of the data protection and privacy regulatory efforts were focused on the US and Europe, in 2014, the African Union adopted the Convention on Cyber Security and Personal Data Protection ("the Malabo Convention"). The Malabo Convention is an important data protection international agreement in Africa, and it aims to establish a legal framework for cybersecurity and data protection within the African Union Member States.

Following the enactment of GDPR in the EU, privacy concerns and awareness grew across the globe and triggered the adoption of respective regulations in many regions or countries.

Gartner estimates that by the end of 2023, 75% of world countries will have enacted a privacy regulation. The ripple effects of GDPR can be felt everywhere. The most notable (or famous) privacy laws include:

- The California Consumer Privacy Act (CCPA) enacted in 2020.
- China's Personal Information Protection Law (PIPL) adopted in 2021.
- The Protection of Personal Information Act (POPIA) in South Africa, which was enforced in July 2020.
- Brazil's Lei Geral de Protecao de Dados (LGPD), or General Data Protection Law, passed in 2018 (shortly after its cousin GDPR).
- Australia's Privacy Principles supplementing the Privacy Act 1988.

The Impact of GDPR on Data Protection

GDPR has altered the data protection landscape, shifting the responsibilities to organizations and companies that must ensure the security of the personal data they collect, hold, and process. This revolution means that all data processing processes must be aligned and harmonized. Securing data under the GDPR must lead to data anonymization to guarantee the confidentiality and integrity of all personal data.

In addition, GDPR imposes obligations on companies to secure their customers' data. These include the encryption of data at rest and in transit, reinforced authentication controls, and measures to access stored data. These obligations are particularly restrictive for companies but have also made it possible to enable and strengthen data security and, beyond that, the cybersecurity of organizations in general.

Through gradual and scalable implementations, GDPR has enabled companies to strengthen their defenses according to the specific needs of each organization.

Above all, GDPR has become the driving force to focus on effective data protection that builds trusted relationships with citizens and customers and enhances user experience. Compliance with GDPR is an enabler of innovation and business growth, having a global impact. GDPR is considered the cornerstone of privacy and data protection regulations and is the foundation of the many laws enacted in countries like Brazil, Japan, China, and India.

Business Benefits of Data Protection

Data and its processing is a core component of any organization's activities, big or small. Here are five reasons why data protection is essential and why it is beneficial for your organization to comply with data protection laws.

1 RESPECT YOUR CUSTOMERS

Data protection is a fundamental human right protected by law.

2 BUILD TRUST WITH YOUR CUSTOMERS

Individuals are increasingly concerned about their digital rights and their right to data protection.

3 IMPROVE YOUR BRANDING

Attract and retain customers by demonstrating compliance.

4 PREVENT FRAUD

Protect the data your organization holds and processes.

5 SAVE TIME AND MONEY

Data breaches can become very costly, disrupting operations, requiring time and resources to mitigate the impact.

1. Respect your customers

Data protection is a fundamental human right protected by the UN Declaration of Human Rights and the EU Charter. The right to data protection is a right that may impact the effectiveness of other fundamental rights, such as freedom of speech. Protecting your customers' data (and your data) proves that you respect their human rights, which has many more benefits.

2. Build trust with your customers

Individuals are increasingly concerned about their digital human rights and their right to data protection. Mismanagement of personal data can damage an organization's public reputation and undermine individuals' trust. It takes years to build trust, but it can be destroyed in seconds. As such, an organization that demonstrates good privacy compliance through robust data protection procedures is more likely to build trust amongst its users or customers.

3. Improve your branding

Individuals trust organizations for the quality of services (and products) they offer. A diligent approach to data protection is a privacy service that customers, partners, and suppliers will appreciate. Robust data protection policies and transparency on how an organization collects, stores, processes, and protects data can help retain existing customers, attract new clientele and contracts, and increase revenue. In addition, data protection is a foundational requirement for getting cyber insurance.

4. Prevent fraud and cybercrime

Data held by companies, including personal data, financial information, medical records, and intellectual property, are a cybercriminal's favorite target because they can easily monetize the stolen data. Applying strong data protection measures and safeguards protects not only individuals' or customers' personal data but also your organization's data. Data protection can help companies avoid considerable problems that may disrupt operations, damage reputation, and incur fines.

5. Save time and money

Dealing with the aftermath of a data breach can be costly and time-consuming. Organizations must spend time contacting individuals affected by this event and could potentially pay fines and legal fees to the individuals concerned. In addition, the cost of a data breach can be further increased, considering the potential disruption of operations and the time and resources required to bring systems and data back to a functional state.

Moving Beyond Compliance

Many organizations think of data protection only in the framework of checking a compliance box. However, compliance is a point in time that does not prove your data is continuously protected. While for some, compliance is a necessary evil, for leaders it is an opportunity for business growth. If organizations want to optimize their data protection processes and technology, data protection must be seen as more than being compliant and cyber resilient. It should be embraced as a tool for growth and achievement.

Follow your Values
Data protection should not be driven solely by extrinsic factors, such as compliance or the sword of Damocles for fines and penalties. These external factors are needed – data protection is required to achieve compliance and avoid security risks. However, for more mature organizations, data protection is more about making a difference in a competitive business and market environment. It is driven by intrinsic values and the ethics of respecting yourself and your customers and partners. When data protection is seen proactively, it becomes a driver of success and achievement.

Privacy by Design

As new consumer privacy regulations arise, merely meeting the minimum requirements reactively will become increasingly expensive. Regulatory environments are unpredictable, and taking a completely reactive approach or treating each law individually can incur significant costs. The challenge lies in the difficulty of retrofitting privacy features into existing products.

Instead, organizations should prioritize proactive compliance by incorporating privacy by design. This entails investing in flexible business competencies and technology capabilities to address multiple needs and promote long-term business agility. These competencies can then be utilized to create new products or services, prioritize data privacy, and build readiness for responding to future regulations.

Build Data Trust

Many companies are increasing their investment in data tools, initiatives, and teams to become "data-driven organizations." However, trust in the reliability and usefulness of the data is essential for stakeholders, consumers, and leaders. Businesses should focus on people, processes, and technology to establish a trustworthy data culture. And the first step toward creating a positive and trustworthy data culture is investing in people.

An Important Aspect of Data Protection: Data Sovereignty

Digital sovereignty has emerged as a pressing topic in Europe and elsewhere. EU leaders have drafted a letter saying, "Now is the time for Europe to be digitally sovereign." Digital sovereignty refers to the ability to control your own digital destiny – the data, hardware, and software you rely on and create.

Digital sovereignty is a major concern due to a few large technology companies controlling vast amounts of user data. Data sovereignty has become a crucial aspect of achieving digital sovereignty.

Data sovereignty means that the laws and regulations of the country or region in which data is collected, processed, and stored apply to that data. This means a company collecting data in France must abide by French data laws, regardless of location. Similarly, if the same company collects data in Canada, it must also comply with Canadian data sovereignty laws.

This adds complexity for businesses operating across international borders regarding data collection and processing. Organizations should carefully consider their options for storing data, particularly in the cloud, considering data residency and privacy requirements while balancing the need for efficiency and competitiveness. Imposing overly strict limitations on data location could hinder innovation, yet the completely free movement of data across jurisdictions poses risks that must be carefully weighed.

Data Protection vs. Data Sovereignty

Maintaining data sovereignty regulations can be challenging when it comes to protecting sensitive data in the cloud. With 79% of global organizations utilizing multiple cloud platforms[1] , ensuring that restricted or classified data and workloads are stored and accessed only by users in specific jurisdictions becomes increasingly essential.

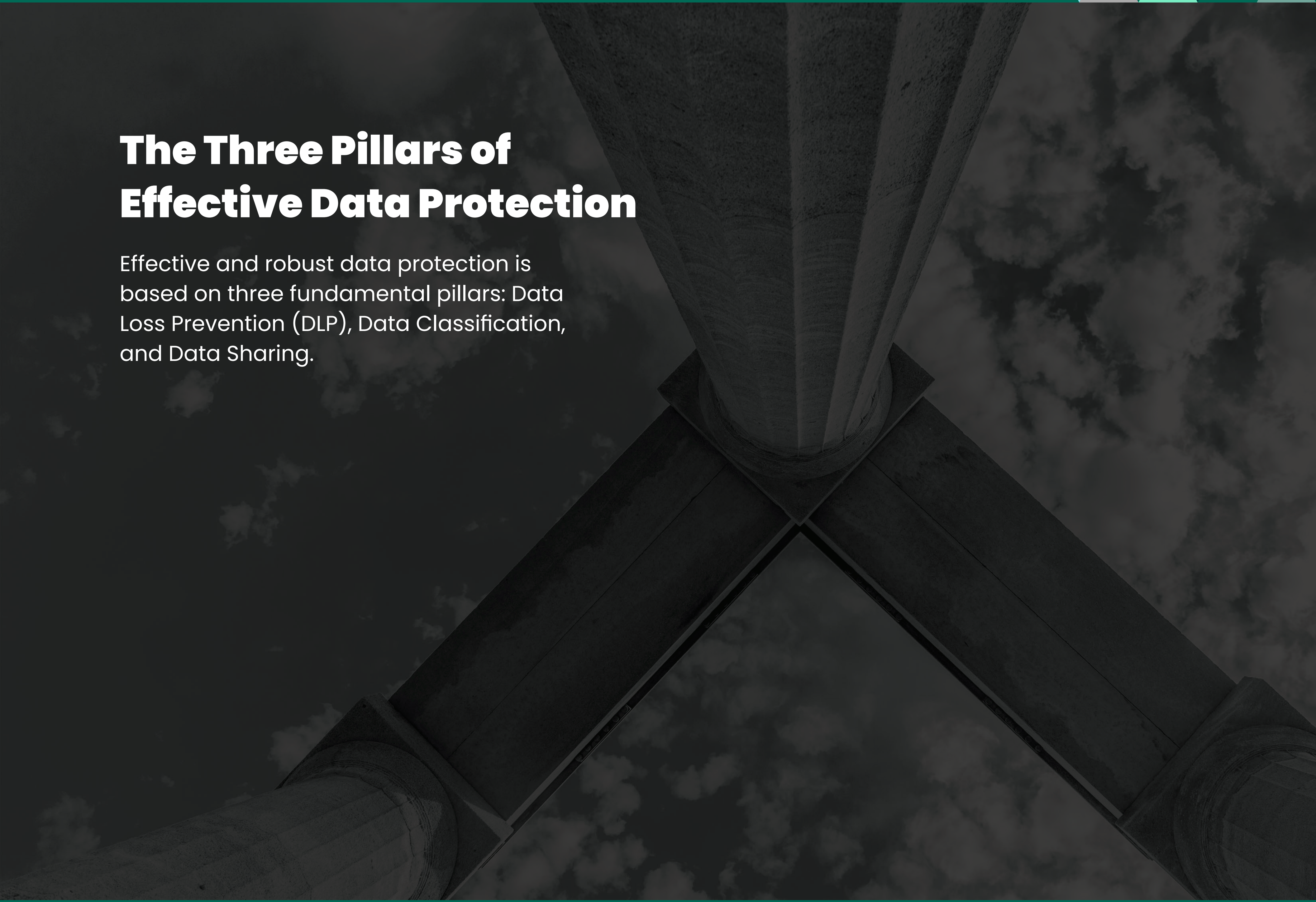
Data protection is a shared responsibility between organizations and cloud providers. Enterprises must take ownership and maintain independent sovereign data protection controls that can operate globally or locally. Adopting a "think globally, act locally" approach can centralize data protection controls for better local enforcement and ensure data sovereignty.

[1] Thales 2023 Data Threat Report, available for download at https://cpl.thalesgroup.com/data-threat-report

10 Questions to Ask Your Data Protection Vendor

With so many vendors offering data protection solutions, selecting the one that will help you meet all business and regulatory requirements becomes challenging. The following questions can help you shortlist these vendors. Cost and support should be considered before reaching a final decision.

1. Can you identify the data you have, structured or unstructured, across platforms, devices, and the cloud?
2. Can you classify your data with rich, actionable metadata?
3. Can you tailor data classification to meet the requirements of applicable privacy and data sovereignty laws and legislations?
4. Does data governance impact experience and productivity?
5. Does the solution provide security warnings that reinforce security awareness training?
6. Does the solution enable secure collaboration?
7. Do the access controls enable a zero-trust approach to data protection?
8. Does the data owner retain control over sensitive data when transferred outside the organization?
9. Can you monitor and log threats to your data?
10. Can you prove regulatory compliance through comprehensive reporting?



The Three Pillars of Effective Data Protection

Effective and robust data protection is based on three fundamental pillars: Data Loss Prevention (DLP), Data Classification, and Data Sharing.

Data Protection and Data Classification

Data classification is necessary to manage risk, ensure compliance, and protect sensitive information. It involves organizing data into relevant categories for more efficient use and safeguarding. Data classification simplifies the process of locating and retrieving data.
The classification process entails tagging data for easy tracking and indexing while eliminating duplicate data entries. This results in reduced storage and backup expenses and faster search times. In terms of data protection, data classification is a valuable tool for implementing appropriate security measures that correspond to the specific type of data being accessed, transmitted, or duplicated.

Data Protection and Secure Collaboration

Data classification is necessary to manage risk, ensure compliance, and protect sensitive information. It involves organizing data into relevant categories for more efficient use and safeguarding. Data classification simplifies the process of locating and retrieving data.
The classification process entails tagging data for easy tracking and indexing while eliminating duplicate data entries. This results in reduced storage and backup expenses and faster search times. In terms of data protection, data classification is a valuable tool for implementing appropriate security measures that correspond to the specific type of data being accessed, transmitted, or duplicated.

Data Protection and Data Loss Prevention

Data loss prevention (DLP) is a set of tools and processes to prevent data compromise, misuse, or unauthorized access. Data loss prevention software and tools monitor and control endpoint activities, filter data streams on corporate networks, and monitor data in the cloud to protect data at rest, in motion, and in use.

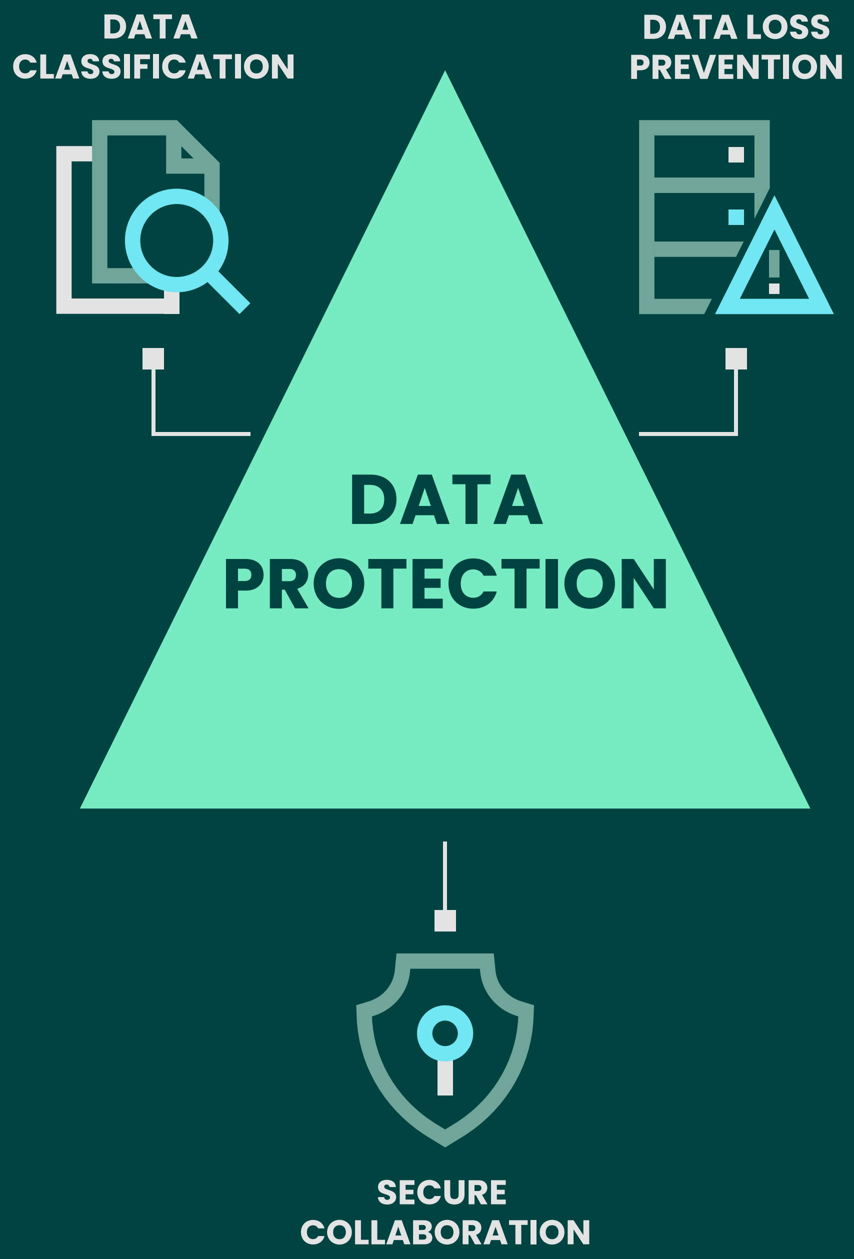
DLP software establishes regulated, confidential, and business-critical data and identifies violations of organizational policies or regulatory compliance requirements such as HIPAA, PCI-DSS, or GDPR. Once those violations are identified, DLP enforces remediation actions to prevent the accidental or malicious disclosure of data that could create organizational risks.

DLP also provides reporting to meet compliance and auditing requirements and identify areas of weakness and anomalies for forensics and incident response.

The Power of Three

Organizations rely on sensitive data to serve customers, fuel innovation, and grow. Security leaders need a way to find and understand that data, protect it from loss or theft while within their extended enterprise, and securely share it outside their extended enterprise.

By combining the powers of data loss prevention, data classification, and secure data sharing, business leaders can afford interlocking security for all cybersecurity maturity levels. Modular solutions for data classification, data loss prevention, and secure collaboration combine to address business needs and use cases and help identify, classify, monitor, and protect your most valuable asset, your data.


DATA CLASSIFICATION

DATA LOSS PREVENTION

DATA PROTECTION

SECURE COLLABORATION

Fortra's Solutions for Data Protection

Fortra offers a comprehensive portfolio of modular and integrated data protection solutions that help businesses identify, classify, control, and protect their data at rest, in motion, and in use.

Fortra's Digital Guardian data loss prevention gives immediate visibility into data security, intuitive results in out-of-the-box dashboards, and greater deployed efficacy. From discovery to monitoring to blocking, comprehensive data loss prevention capabilities help support compliance initiatives and protect against serious risk while guiding users on the next-best security step. SaaS and Managed Service deployment options help deliver results faster and offer the expertise businesses need.

Fortra's Data Classification Suite solution enhances data security by applying visual and metadata labels to best support DLP policies. AI engine recommendations help reduce business friction by guiding which label is best to apply, and employees receive real-world security training that drives visibility and engagement with data security practices across the organization.

Digital Guardian Secure Collaboration solution encrypts and controls access to sensitive files wherever they go. Taking a Zero-Trust approach to file sharing, collaboration with anyone – external or internal – is always quick and secure, with the option to revoke access instantly.

Glossary

As with all aspects of cybersecurity, a lot of jargon is often thrown around when discussing data protection. While by no means a comprehensive list, here are a few key terms worth remembering.

Data at rest – Data that is stored and is not accessed or used. The term excludes data moving across networks or temporarily in computer memory waiting to be processed.

Data in motion - Also referred to as data in transit, this is data transported between locations within or between computing systems.

Data in use – Data currently being updated, processed, erased, accessed, or read by a system.

Data Culture - The collective behaviors, assumptions, and beliefs of an organization's employees who share a common understanding of using corporate data for decision-making and operations in a way that is compliant with internal policies and external regulations.

Intellectual Property – A broad category of intangible (i.e., non-physical) assets owned and legally protected by a company or individual from unauthorized external use or processing without consent. Examples of intellectual property (IP) include patents and inventions; literary and artistic works; industrial designs; and symbols, brand names, and logos.

Personal Data - Any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data[2]. In the US legislation, personal data is referred to as Personally Identifiable Information (PII).

Data Governance – Everything an organization does to ensure data is secure, private, accurate, available, and usable. It includes the actions people must take, the processes they must follow, and the technology that supports them throughout the data life cycle[3] .

Zero Trust – A security framework that requires strict identity validation and verification for every person and device requesting authorization to access resources on a corporate network. Zero Trust is based on the premise "always validate, never trust" and considers that every entity, whether sitting within or outside the network perimeter, is untrusted.

Structured Data - Data with a standardized format for efficient access and analysis by software and humans alike.

Unstructured Data - Unstructured data is information that is not arranged according to a preset data model or schema and, therefore, cannot be stored in traditional databases. Most business documents, such as email messages, videos, photos, webpages, and audio files, are unstructured.

[2] Official definition included in GDPR, available at https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

[3] Definition offered by Google at https://cloud.google.com/learn/what-is-data-governance

FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

|