Data Topics

Analytics | Database | Data Architecture | Data Literacy | Data Science | Data Strategy | Data Modeling | EIM | Governance & Quality | Smart Data

Homepage > Education Resources For Use & Management of Data > What is...? > What Is Data Privacy? Definition, Benefits, Use Cases

What Is Data Privacy? Definition, Benefits, Use Cases

By **Michelle Knight** on **April 17, 2024**

Shutterstock

Data privacy describes a set of principles and guidelines to ensure the respectful processing, protection, and handling of sensitive data linked to a person. This concept ties to who can define, observe, use, and control a person's information and how.

Typically, privacy spans two types of levels: implicit rules and written legislation. Implicit rules cover norms, behaviors, and values about confidentiality that people understand but don't necessarily state.

The specifics differ depending on culture, social needs, and regulations. But, general principles exist as noted by the Organization for Economic Co-operation and Development (OECD), ng :

- Allowing individuals to challenge data accuracy related to him, her, or they
- Holding organizations accountable for following these guidelines

As technology has progressed rapidly, customers hold corporations in good faith by following these principles. However, increasing confusion, data breaches, and abuses in the 2000s and 2010 prompted governments to step in.

Consequently, data privacy legislation spans over 120 countries .

Data Privacy Defined

Many data privacy definitions emphasize compliant behavior according to local laws, regulations, and standards. As new technologies and regulations emerge , firms must be aware of them when building their capabilities.

Other descriptions highlight the trust provided by providers to consumers. Many organizations actively promote trust by demonstrating transparency and using automation to handle privacy requests.

The ability to control personal data is another common concept expressed when describing data privacy. IBM specifies that information privacy embraces “the principle that a person should have control over their data.” Access control and consent management feature prominently in the definition of data privacy, especially when discussing software.

Security represents another central idea when other sources define data privacy. Corporate Compliance Insights connects data privacy with stringent and robust cybersecurity responses.

A Cisco study states that 94% of respondents believed that customers would not remain without adequate data privacy protection. Compliance, trust, control, and security underlie fundamental data privacy concepts.

Data Privacy vs. Data Security

Data privacy intersects with data security in the protecting personal information. For example, if a financial institution tightens the security of its digital access, individual account information data privacy.

Data security has a different meaning. It assumes that some other entity wants to get information without access or agreement from the owner. So, organizations need a physical infrastructure and business operations that safeguard personal information from unauthorized access.

Data security underlies a critical corporate capability to prevent data breaches and protect information. To learn more, visit the data privacy vs. data security article.

The Evolution of Data Privacy and Its Legislation

Data privacy, as a concept, started long before the first personal computers in the 1970s . The idea became law in many constitutions and the U.S. Bill of Rights in 1789.

As information technology advanced, personal data became easier to transmit. The 1990s saw the European Union's (EU) Data Protection Directive. The US passed specific privacy regulations like the Health Insurance Portability and Accountability Act (HIPAA) and the US's financial sector's Gramm–Leach–Bliley Act (GLBA).

In 2018, the EU enacted the General Data Protection Regulation (GDPR) . This law formalized the need for clear permissions before using a person's data and became a foundation for greater data protection legislation.

While the U.S. lacks a comprehensive federal law, 15 individual states have privacy regulations, with California leading the way with the California Consumer Privacy Act (CCPA). Worldwide, laws continue to expand to encompass artificial intelligence or AI, with the EU's AI Act passed in 2024.

Types of Data Covered

Data privacy covers specific types of data that identify an individual. In contrast, anonymized data, such as the main email of the local water bureau, does not require data privacy protections and is considered public. With the rise of big data usage, especially through AI and cloud cuting, companies mask data through data anonymization.

number, birthday, or place of birth.

- **Personal Information (PI):** PI information encompasses all PII data and data that could be linked directly or indirectly to a consumer or household. Examples of PI data that are not PII data include IP addresses, locations, photographs, and criminal information.
- **Sensitive Personal Information**: Sensitive personal data could be linked to an individual with other data and lead to harm. For instance, a person may select religion from a choice of options. Tracing back this data to someone could put them in danger of a hate crime.

While these three confidential data types make up most of the information requiring safe processing, different contexts, locations, and industries require additional protections. For example, keeping children's voice recordings indefinitely and failing to provide an adequate mechanism to delete that data violates the U.S. Children's Online Privacy Protection Rule.

This activity resulted in a lawsuit with the company, Amazon. However, a company could keep adult voice recordings indefinitely unless a person requests to delete their information with consent. When unsure whether to secure data, consult the data owner or an expert in data privacy regulations for advice.

Why Data Governance Is Key to Handling Data Privacy

Data Governance is critical in handling data privacy as it is a business program that formalizes harmonized data activities across the organization. Discussions about standards, processes, and practices clarify departmental viewpoints and reasoning in the company, which leads to understanding and agreement about business operations demonstrating data privacy.

Additionally, Data Governance supports access to personal data with a customer's permission. For example, if someone calls a bank about a suspected fraudulent charge, the associate will ask to access personally identifiable information for investigation. Data privacy relies on the safety of this interchange and its shareability to do business.

This interactive governance component is very important and often overlooked by businesses. For example, Amazon used worker handheld scanners not only to track inventory but to monitor employee activity without their workers' consent . In early 2024, a French regulator fined the company about $34.7 million.

This case shows how easily technology allocated for a sensible business purpose can extend to additional problems without considering the privacy implications. With a solid Data Governance

- Organizations contribute to Data Privacy Day events on January 28th to educate consumers and businesses about ways to manage personally identifiable information better.
- Portland, Oregon, is creating a surveillance technology inventory in response to a city audit that noticed privacy gaps during protests. As part of a resolution, the surveillance information will respect privacy by being more transparent with residents about the data it collects and uses.
- Growing concerns about privacy and regulations have led Google to phase out third-party cookies , which track browsing activities and preferences as part of web advertising. In 2024, Google expects third-party cookies to end.
- As a convention , users do not share their passwords with another person to protect privacy. This practice is routine. Managers who find workers sharing their passwords have fired them.
- Organizations need to train AI models to identify fraudulent transaction activity but in real-life, this data is sensitive. So, organizations develop and substitute synthetic data that simulates these financial crimes. This approach respects data privacy while increasing system security.

Benefits of Data Privacy

Respecting data privacy provides businesses with many benefits, including:

- **Trust with Customers:** Businesses want their clients to return for additional products and services. Clients demand data protection, with 79% saying it underlies their trust in companies and more than 80% would stop doing business with a company that had a data breach.
- **Legal Compliance:** The number of class action suits and fines for non-compliance with data privacy regulations has risen over the last couple of years. Firms must handle personal and sensitive data well to avoid spending time in court and losing money.
- **Risk Management:** Organizations do well when business operations run as expected and enter panic mode when they no longer control their data. Taking precautions around data privacy increases organizational confidence in processes and activities.
- **Prospective Clients Become Customers:** Companies need to stand out positively in a competitive marketplace with dwindling economic resources. A company that demonstrates transparency and trust could attract 56% of mistrustful initial contacts. Whereas 44% of consumers are most comfortable sharing financial or health

DATAVERSITY.net TDAN.com

Conferences

Enterprise Data World

Data Governance & Information Quality

Online Conferences

Enterprise Data Governance Online

Data Architecture Online

DATAVERSITY Resources

DATAVERSITY Training Center

Women in Data Management and Governance

White Papers

Product Demos

What is...?

Data Puppets

Company Information

Why Train with DATAVERSITY

About Us

Content Sponsorship

Contact Us

Press Room

Newsletters

DATAVERSITY Weekly

Women in Data Management and Governance Monthly Newsletter

TDAN Bimonthly Newsletter

DATAVERSITY Email Preferences

DATAVERSITY Education

Data Conferences

Trade Journal

Online Training

Upcoming Live Webinars

Cookies Settings

CA: Do Not Sell My Personal Information Privacy Policy Terms of Service