
DATA
PRIVACY

WHAT IS DATA PRIVACY?

SkillToPro

Data Privacy or Information Privacy is a part of the data protection area that deals with the proper handling of data focusing on compliance with data protection regulations.

Data Privacy is centered around how data should be **collected, stored, managed, and shared** with any third parties, as well as compliance with the applicable privacy laws (such as the California Consumer Privacy Act-CCPA or General Data Protection Regulation GDPR).

DATA PRIVACY VS DATA SECURITY

SkillToPro

Data Privacy

Compliance with data protection laws and regulations. Focus on how to collect, process, share, archive and delete the data

≠

Data Security

Measures that an organzation is taking in order to prevent any third party from unauthorized access.

Data Privacy Manager

TYPES OF PRIVATE INFORMATION

Private information may come in many forms. Two of the most common elements of private information are **Personally Identifiable Information** and **Protected Health Information**:

- **Personally identifiable information (PII)** includes all information that can be tied back to a specific individual.
- **Protected health information (PHI)** includes health care records that are regulated under the Health Insurance Portability and Accountability Act (HIPAA).

EXPECTATION OF PRIVACY

- The **reasonable expectation of privacy** is an essential element of privacy law. We sometimes refer to privacy as the ***"right to be left alone."*** You might wonder: When do I have the right to privacy? In what places do I have the right? What circumstances or which activities give me a legal right to privacy?

- The **Reasonable Expectation Of Privacy** allows you to hold someone accountable for violating your personal privacy. When another party unreasonably interferes with your desire to keep your personal matters away from the public, the court can hold them liable for their intrusion.

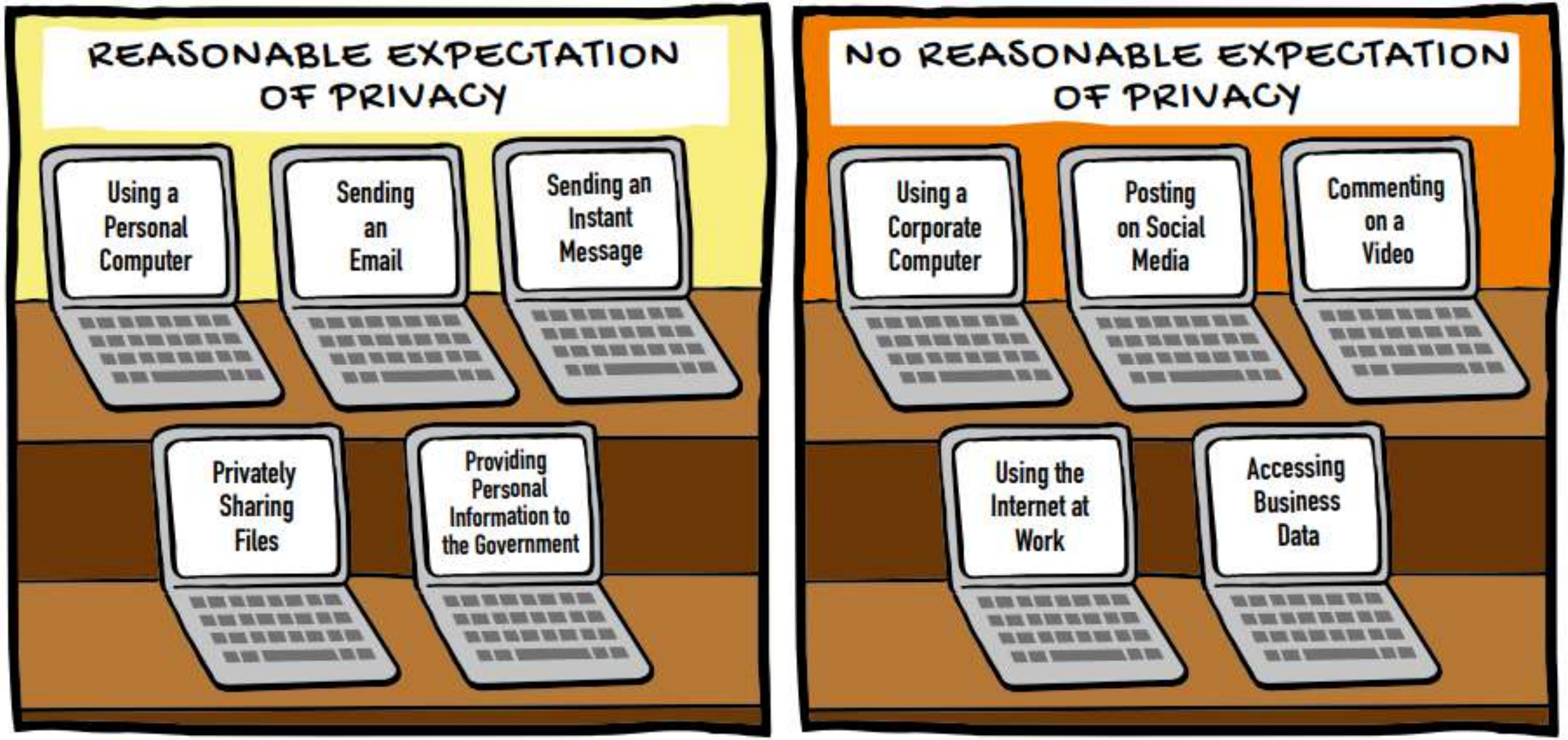
EXPECTATION OF PRIVACY

SkillToPro

- When you put content on social media, whether it be a post on a social networking site or a comment on a shared video, **you generally have no reasonable expectation of privacy.** You're posting that content publicly or to a large group of people, and a reasonable person would assume that is not a private conversation.
- When you're using a computer or network that belongs to your employer, you generally **do not have a reasonable expectation of privacy.** The employer owns that equipment and is normally legally entitled to monitor the use of their systems.
- As a **cybersecurity professional**, **you should communicate to users clearly and accurately about their privacy expectations**. It's important to reinforce that when employees of your organization are using systems or networks that belong to the organization, they should not have an expectation of privacy.

EXPECTATION OF PRIVACY

SkillToPro



DATA PRIVACY PROGRAM

SkillToPro

- A **data privacy program** serves as the framework through which you can find solutions to data privacy problems.
- **It's the collection of approaches, processes, and tools that you use to protect the privacy of your customers, employees, partners, and other stakeholders**.
- Ultimately, it improves your organization's ability to collect, process, and store personal information in a way that complies with the relevant data privacy laws.
- Data privacy programs will differ from organization to organization, as every organization works with personal information in different ways.

ELEMENTS OF A DATA PRIVACY PROGRAM

1. Notices
2. Data Inventories and/or Records of Processing Activities
3. Privacy Impact Assessments
4. Privacy Incident and Breach Response
5. Resourcing
6. Privacy Awareness and Training
7. Privacy Culture
8. Consent Management
9. Subject Rights Request Management
10. Data Minimization and Purpose Limitation
11. Contract Management
12. Vendor Risk Management
13. Security Controls
14. Privacy by Design
15. Governance and Accountability
16. Program Management

PRIVACY MANAGEMENT FRAMEWORK

- The Privacy Management Framework (PMF) is an attempt to establish a global framework for privacy management. The PMF includes nine principles that were developed by the American Institute of Certified Public Accountants (AICPA) with subject matter expert input.

The **Nine PMF Principles** are as follows:

1. **Management** - The entity defines, formally documents, communicates, and assigns accountability for its PI (personal information) privacy policies and procedures.
2. **Agreement, Notice, and Communication** - The entity makes formal agreements, notifies and communicates with and offers choices when seeking data subject consents, including reasons why and purposes for which the entity seeks to obtain and use a data subject's PI.

PRIVACY MANAGEMENT FRAMEWORK

3. **Collection and Creation** - The entity collects and creates PI only for the purposes identified in its agreements with data subjects, and in ongoing communications with and notices provided to data subjects.
4. **Use, Retention, and Disposal** - The entity limits the use of PI to the purposes identified in the formal agreements/notices, and for which a data subject has provided explicit (or implicit) consent. The entity retains PI for the time necessary to fulfill the stated purposes identified in the formal agreements/notices or as required by laws or regulations. Once those purposes have been met, the entity securely disposes of the information.
5. **Access** - The entity provides data subjects with access to their PI when requested or when asked to update and correct data errors or make changes.

PRIVACY MANAGEMENT FRAMEWORK

6. **Disclosure to Third Parties** - The entity discloses PI to third parties only for the purposes identified in data subject privacy agreements and its privacy notice and with the explicit consent of the data subject.
7. **Security for Privacy** - The entity protects PI against unauthorized access, removal, alteration, destruction and disclosure (both physical and logical).
8. **Data Integrity and Quality** - The entity maintains accurate, complete and relevant PI for the purposes identified in the notice and protects the representational integrity of the PI in its ongoing interactions with data subjects.
9. **Monitoring and Enforcement** - The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

DATA PRIVACY – USE CASE

An example of data privacy in action:

- Consider a budgeting app that people use to track spending and other sensitive financial information. When a user signs up, the app displays a privacy notice that clearly explains the data it collects and how it uses that data. The user can accept or reject each use of their data individually.

- For example, they can decline to have their data shared with third parties while allowing the app to generate personalized offers.

- The app heavily encrypts all user financial data. Only administrators can access customer data on the backend. Even then, the admins can only use the data to help customers troubleshoot account issues, and only with the user's explicit permission.

DATA PRIVACY – USE CASE

This example illustrates three core components of common data privacy frameworks:

- **Complying with regulatory requirements:** By letting users granularly control how their data is processed, the app complies with consent rules that are imposed by laws like the California Consumer Privacy Act (CCPA).
- **Deploying privacy protections:** The app uses encryption to protect data from cybercriminals and other prying eyes. Even if the data is stolen in a cyberattack, hackers can't use it.
- **Mitigating privacy risks:** The app limits data access to trusted employees who need it for their roles, and employees can access data only when they have a legitimate reason to. These access controls reduce the chances that the data is used for unauthorized or illegal purposes.

DATA PRIVACY LAWS

Compliance with relevant regulations is the foundation of many data privacy efforts. ***While data protection laws vary, they generally define the responsibilities of organizations that collect personal data and the rights of the data subjects who own that data.***

The General Data Protection Regulation (GDPR)

The **GDPR is a European Union privacy regulation** that governs how organizations in and outside of Europe handle the personal data of EU residents. In addition to being perhaps the most comprehensive privacy law, it is among the strictest**. Penalties for noncompliance** can reach up to **EUR 20,000,000 or 4% of the organization's worldwide revenue in the previous year, whichever is higher. Links:** https://gdpr-info.eu , https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/, https://gdpr.eu

The UK Data Protection Act 2018

The **Data Protection Act 2018** is, essentially, the UK's version of the GDPR. It replaces an earlier data protection law and implements many of the same rights, requirements, and penalties as its EU counterpart.

DATA PRIVACY LAWS

SkillToPro

The Personal Information Protection and Electronic Documents Act (PIPEDA)

Canada's PIPEDA governs how private-sector businesses collect and use consumer data. PIPEDA grants data subjects a significant amount of control over their data, but it applies only to data used for commercial purposes. Data used for other purposes, like journalism or research, is exempt.

US data protection laws

Many individual US states have their own data privacy laws. The most prominent of these is the **California Consumer Privacy Act (CCPA),** which applies to virtually any organization with a website because of the way it defines the act of "doing business in California."

The ***CCPA empowers Californians to prevent the sale of their data and have it deleted at their request, among other rights***. Organizations face fines of up to USD 7,500 per violation. The price tag can add up quickly. If a business were to sell user data without consent, each record it sells would count as one violation.

DATA PRIVACY LAWS

The US has no broad data privacy regulations at a national level, but it does have some more targeted laws.

Under the **Children's Online Privacy Protection Act (COPPA),** organizations must obtain a parent's permission before collecting and processing data from anyone under 13. Rules for handling children's data became even stricter in the **Kids Online Safety Act (KOSA).** KOSA would require online services to default to the highest privacy settings for users under 18.
Link: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

The **Health Insurance Portability and Accountability Act (HIPAA)** is a federal law that deals with how healthcare providers, insurance companies, and other businesses safeguard personal health information.
Link: https://www.ncbi.nlm.nih.gov/books/NBK500019/

DATA PRIVACY STANDARD

The Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is not a law, but a set of standards developed by a consortium of credit card companies, including Visa and American Express. These standards outline how businesses must protect customers' payment card data.

While the PCI DSS isn't a legal requirement, credit card companies and financial institutions can fine businesses that fail to comply or even prohibit them from processing payment cards.

https://www.pcisecuritystandards.org

DATA PRIVACY PRINCIPLES AND PRACTICES

Some common principles and practices organizations use to bolster data privacy include:

Data Visibility

For effective data governance, an organization needs to know the types of data it has, where the data resides, and how it is used.

Some kinds of data, like biometrics and social security numbers, require stronger protections than others. Knowing how data moves through the network helps track usage, detect suspicious activity, and put security measures in the right places.

Finally, full data visibility makes it easier to comply with data subjects' requests to access, update, or delete their information. If the organization doesn't have a complete inventory of data, it might unintentionally leave some user records behind after a deletion request.

Use Case: A digital retailer catalogs all the different kinds of customer data it holds, like names, email addresses, and saved payment information. It maps how each type of data moves between systems and devices, who has access to it (including employees and third parties), and how it is used. Finally, the retailer classifies data based on sensitivity levels and applies appropriate controls to each type. The company conducts regular audits to keep the data inventory up to date.

DATA PRIVACY PRINCIPLES AND PRACTICES

SkillToPro

User Control

Organizations can limit privacy risks by granting users as much control over data collection and processing as possible. If a business always gets a user's consent before doing anything with their data, it's hard for the company to violate anyone's privacy.

That said, organizations must sometimes process someone's data without their consent. In those instances, the company should make sure that it has a valid legal reason to do so, like a newspaper reporting on crimes that perpetrators would rather conceal.

Example: A social media site creates a self-service data management portal. Users can download all the data they share with the site, update or delete their data, and decide how the site can process their information.

DATA PRIVACY PRINCIPLES AND PRACTICES

SkillToPro

Data Limitation

It can be tempting to cast a wide net, but the more personal data a company collects, the more exposed it is to privacy risks. Instead, organizations can adopt the ***principle of limitation: identify a specific purpose for data collection and collect the minimum amount of data needed to fulfill that purpose.***

Retention policies should also be limited. The organization should dispose of data as soon as its specific purpose is fulfilled.

***Example*:** A public health agency is investigating the spread of an illness in a particular neighborhood. The agency does not collect any PII from the households it surveys. It records only whether anyone is sick. When the survey is complete and infection rates determined, the agency deletes the data.

DATA PRIVACY PRINCIPLES AND PRACTICES

SkillToPro

Transparency

Organizations should keep users updated about everything they do with their data, including anything their third-party partners do.

***Example*:** A bank sends annual privacy notices to all of its customers. These notices outline all the data that the bank collects from account holders, how it uses that data for things like regulatory compliance and credit decisions, and how long it retains the data. The bank also alerts account holders to any changes to its privacy policy as soon as they are made.

Access control

Strict access control measures can help prevent unauthorized access and use. Only people who need the data for legitimate reasons should have access to it. Organizations should use multi-factor authentication (MFA) or other strong measures to verify users' identities before granting access to data. Identity and access management (IAM) solutions can help enforce granular access control policies across the organization.

***Example*:** A technology company uses role-based access control policies to assign access privileges based on employees' roles. People can access only the data that they need to carry out core job responsibilities, and they can only use it in approved ways. For example, the head of HR can see employee records, but they can't see customer records. Customer service representatives can see customer accounts, but they can't see customers' saved payment data.

DATA PRIVACY PRINCIPLES AND PRACTICES

SkillToPro

Data Security Measures

Organizations must use a combination of tools and tactics to protect ***data at rest, in transit, and in use.***

Example: A healthcare provider encrypts patient data storage and uses an intrusion detection system to monitor all traffic to the database. It uses a data loss prevention (DLP) tool to track how data moves and how it is used. If it detects illicit activity, like an employee account moving patient data to an unknown device, the DLP raises an alarm and cuts the connection.

Privacy Impact Assessments

Privacy Impact Assessments (PIAs) determine how much risk a particular activity poses to user privacy. PIAs identify how data processing might harm user privacy and how to prevent or mitigate those privacy concerns.

Example: A marketing firm always conducts a PIA before every new market research project. The firm uses this opportunity to clearly define processing activities and close any data security gaps. This way, the data is only used for a specific purpose and protected at every step. If the firm identifies serious risks it can't reasonably mitigate, it retools or cancels the research project.

DATA PRIVACY PRINCIPLES AND PRACTICES

SkillToPro

Data Privacy by Design and by Default

Data privacy by design and by default is the philosophy that privacy should be a ***core component of everything the organization does—every product it builds and every process it follows. The default setting for any system should be the most privacy-friendly one.***

Example: When users sign up for a fitness app, the app's privacy settings automatically default to "don't share my data with third parties." Users must change their settings manually to allow the organization to sell their data.

DATA PRIVACY VIOLATIONS AND RISKS

Complying with data protection laws and adopting privacy practices can help organizations avoid many of the biggest privacy risks. Some of the most common causes and contributing factors of privacy violations that companies need to look out for are:

Lack of Network Visibility

When organizations don't have complete visibility of their networks, privacy violations can flourish in the gaps. Employees might move sensitive data to unprotected shadow IT assets. They might regularly use personal data without the subject's permission because supervisors lack the oversight to spot and correct the behavior. Cybercriminals can sneak around the network undetected.

As corporate networks grow more complex—mixing on-premises assets, remote workers, and cloud services—it becomes harder to track data throughout the IT ecosystem. Organizations can use tools like attack surface management solutions and data protection platforms to help streamline the process and secure data wherever it resides.

DATA PRIVACY VIOLATIONS AND RISKS

SkillToPro

AI and Automation

Some regulations set special rules for automated processing. For example, the GDPR gives people the right to contest decisions made through automated data processing.

The rise of generative artificial intelligence can pose even thornier privacy problems. Organizations cannot necessarily control what these platforms do with the data they put in. Feeding customer data to a platform like ChatGPT might help garner audience insights, but the AI may incorporate that data into its training models. If data subjects didn't consent to have their PII used to train an AI, this constitutes a privacy violation.

Organizations should clearly explain to users how they process their data, including any AI processing, and obtain subjects' consent. However, even the organization may not know everything the AI does with its data. For that reason, businesses should consider working with AI apps that let them retain the most control over their data.

DATA PRIVACY VIOLATIONS AND RISKS

SkillToPro

Overprovisioned Accounts

Stolen accounts are a prime vector for data breaches, according to the IBM Cost of a Data Breach report. Organizations tempt fate when they give users more privileges than they need. The more access permissions that a user has, the more damage a hacker can do by hijacking their account.

Organizations should follow the principle of least privilege. Users should have only the minimum amount of privilege they need to do their jobs.

Human Error

Employees can accidentally violate user privacy if they are unaware of the organization's policies and compliance requirements. They can also put the company at risk by failing to practice good privacy habits in their personal lives.

For example, if employees overshare on their personal social media accounts, cybercriminals can use this information to craft convincing spear phishing and business email compromise attacks.

DATA PRIVACY VIOLATIONS AND RISKS

SkillToPro

Data Sharing

Sharing user data with third parties isn't automatically a privacy violation, but it can increase the risk. The more people who have access to data, the more avenues there are for hackers, insider threats, or even employee negligence to cause problems.

Moreover, unscrupulous third parties might use a company's data for their own unauthorized purposes, processing data without subject consent.

Organizations should ensure that all data-sharing arrangements are governed by legally binding contracts that hold all parties responsible for the proper protection and use of customer data.

Malicious Hackers

PII is a major target for cybercriminals, who can use it to commit identity theft, steal money, or sell it on the black market. Data security measures like encryption and DLP tools are as much about safeguarding user privacy as they are about protecting the company's network.

DATA PRIVACY OFFICER JOB TITLE HIERARCHY

Data Privacy Analyst

- Data Protection Analyst
- Junior Data Privacy Officer
- Privacy Compliance Assistant

Data Privacy Specialist

- Data Protection Specialist
- Data Privacy Consultant
- Privacy Program Analyst

Senior Data Privacy Officer

- Lead Data Privacy Analyst
- Data Privacy Manager
- Data Protection Officer (DPO)

Data Privacy Team Lead

- Head of Data Privacy
- Principal Data Privacy Consultant
- Data Privacy Governance Manager

Director of Data Privacy

- VP of Data Privacy
- Chief Privacy Officer (CPO)
- Global Data Privacy Lead