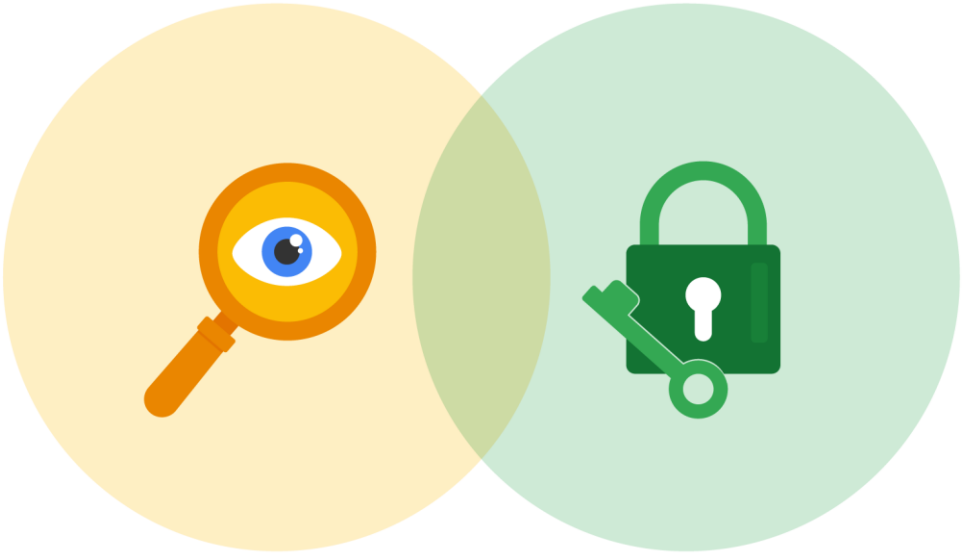
Information privacy: Regulations and compliance

Security and privacy have a close relationship. As you may recall, people have the right to control how their personal data is collected and used. Organizations also have a responsibility to protect the information they are collecting from being compromised or misused. As a security professional, you will be highly involved in these efforts.

Previously, you learned how regulations and compliance reduce security risk. To review, refer to the reading about how security controls, frameworks, and compliance regulations

are used together to manage security and minimize risk. In this reading, you will learn how information privacy regulations affect data handling practices. You'll also learn about some of the most influential security regulations in the world.



Information security vs. information privacy

Security and privacy are two terms that often get used interchangeably outside of this field. Although the two concepts are connected, they represent specific functions:

- **Information privacy** refers to the protection of unauthorized access and distribution of data.
- **Information security** (InfoSec) refers to the practice of keeping data in all states away from unauthorized users.

The key difference: Privacy is about providing people with control over their personal information and how it's shared. Security is about protecting people's choices and keeping their information safe from potential threats.

For example, a retail company might want to collect specific kinds of personal information about its customers for marketing purposes, like their age, gender, and location. How this

private information will be used should be disclosed to customers before it's collected. In addition, customers should be given an option to opt-out if they decide not to share their data.

Once the company obtains consent to collect personal information, it might implement specific security controls in place to protect that private data from unauthorized access, use, or disclosure. The company should also have security controls in place to respect the privacy of all stakeholders and anyone who chose to opt-out.

Note: Privacy and security are both essential for maintaining customer trust and brand reputation.

Why privacy matters in security

Data privacy and protection are topics that started gaining a lot of attention in the late 1990s. At that time, tech companies suddenly went from processing people's data to storing and using it for business purposes. For example, if a user searched for a product online, companies began storing and sharing access to information about that user's search history with other companies. Businesses were then able to deliver personalized shopping experiences to the user for free.

Eventually this practice led to a global conversation about whether these organizations had the right to collect and share someone's private data. Additionally, the issue of data security became a greater concern; the more organizations collected data, the more vulnerable it was to being abused, misused, or stolen.

Many organizations became more concerned about the issues of data privacy. Businesses became more transparent about how they were collecting, storing, and using information. They also began implementing more security measures to protect people's data privacy. However, without clear rules in place, protections were inconsistently applied.

Note: The more data is collected, stored, and used, the more vulnerable it is to breaches and threats.

Notable privacy regulations

Businesses are required to abide by certain laws to operate. As you might recall, **regulations** are rules set by a government or another authority to control the way something is done. Privacy regulations in particular exist to protect a user from having their information collected, used, or shared without their consent. Regulations may also describe the security measures that need to be in place to keep private information away from threats.

Three of the most influential industry regulations that every security professional should know about are:

- General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)

GDPR

GDPR is a set of rules and regulations developed by the European Union (EU) that puts data owners in total control of their personal information. Under GDPR, types of personal information include a person's name, address, phone number, financial information, and medical information.

The GDPR applies to any business that handles the data of EU citizens or residents, regardless of where that business operates. For example, a US based company that handles the data of EU visitors to their website is subject to the GDPRs provisions.

PCI DSS

PCI DSS is a set of security standards formed by major organizations in the financial industry. This regulation aims to secure credit and debit card transactions against data theft and fraud.

HIPAA

HIPAA is a U.S. law that requires the protection of sensitive patient health information. HIPAA prohibits the disclosure of a person's medical information without their knowledge and consent.

Note: These regulations influence data handling at many organizations around the world even though they were developed by specific nations.

Several other security and privacy compliance laws exist. Which ones your organization needs to follow will depend on the industry and the area of authority. Regardless of the circumstances, regulatory compliance is important to every business.

Security assessments and audits

Businesses should comply with important regulations in their industry. Doing so validates that they have met a minimum level of security while also demonstrating their dedication to maintaining data privacy.

Meeting compliance standards is usually a continual, two-part process of security audits and assessments:

- A **security audit** is a review of an organization's security controls, policies, and procedures against a set of expectations.
- A **security assessment** is a check to determine how resilient current security implementations are against threats.

For example, if a regulation states that multi-factor authentication (MFA) must be enabled for all administrator accounts, an audit might be conducted to check those user accounts for compliance. After the audit, the internal team might perform a security assessment that determines many users are using weak passwords. Based on their assessment, the team could decide to enable MFA on all user accounts to improve their overall security posture.

Note: Compliance with legal regulations, such as GDPR, can be determined during audits.

As a security analyst, you are likely to be involved with security audits and assessments in the field. Businesses usually perform security audits less frequently, approximately once per year. Security audits may be performed both internally and externally by different third-party groups.

In contrast, security assessments are usually performed more frequently, about every three-to-six months. Security assessments are typically performed by internal employees, often as preparation for a security audit. Both evaluations are incredibly important ways to ensure that your systems are effectively protecting everyone's privacy.

Key takeaways

A growing number of businesses are making it a priority to protect and govern the use of sensitive data to maintain customer trust. Security professionals should think about data and the need for privacy in these terms. Organizations commonly use security assessments and audits to evaluate gaps in their security plans. While it is possible to overlook or delay addressing the results of an assessment, doing so can have serious business consequences, such as fines or data breaches.