

SecurityAwarenessNews

the security awareness newsletter for security aware people



Data Privacy & Compliance

- The What, Why, and How of Compliance Regulations
- Regulations and Responsibilities
- The Value of Personal Data

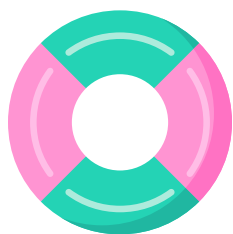


The What, Why, and How of Compliance Regulations



What are data compliance regulations?

In terms of data privacy and security, regulatory compliance refers to guidelines that organizations must follow when collecting, handling, and transferring an individual's personal data. Said data could include full names, addresses, health records, financial information, race, sex, and almost anything that identifies a specific person.



Why do these regulations exist?

The main goal of compliance is to balance an organization's need to collect data with an individual's right to privacy. Without regulations, there would be no standardization for providing adequate security, and there would be no recourse for us as individuals should an entity improperly access or transfer our personal information.



How do regulations help improve security and privacy?

Many regulations require data collectors to implement security policies and robust practices for how data is handled. Failure to comply could result in fines and legal action, which incentivizes organizations to ensure their processes align with applicable regulations and laws.



What's your role in all of this?

We don't expect you to be a compliance expert. But we do expect you to ensure that our organization avoids any potential regulatory violations, which begins with following policy. Similar to regulations, our policies set specific guidelines for how we collect, store, and handle data. Failure to follow policy—intentionally or unintentionally—immediately threatens our commitment to keeping confidential information confidential.









Regulations and Responsibilities

There are many different regulatory standards worldwide that vary by location and industry. The European General Data Protection Regulation (GDPR), for example, is often referred to as the gold standard in compliance due to its comprehensive privacy and security requirements for collecting data of European citizens. Some countries—like Japan, Canada, and Brazil—have laws similar to the GDPR, while others, such as the United States, have no single data protection law and instead divide regulations into specific sectors (such as healthcare, finance, and education).

Regardless of scope or location, all data compliance regulations share common goals: develop standards for data privacy, increase the rights of individuals to control their personal data, and penalize organizations that fail to comply.

And while those goals are a vital part of privacy, they don't actually secure data. Similar to how speed limits can't control how fast people drive, compliance regulations can't prevent people from clicking on phishing links. They can't ensure systems and devices are regularly updated. They can't implement strong, unique passwords.

Those responsibilities are on us—the individuals who have access to confidential information. Every member of our organization plays a fundamental role in ensuring we adhere to the compliance regulations that apply to us by protecting the data we collect. Here's how you can help:

-  **Don't get phished.** Malicious links and attachments often carry malware that is designed to steal data.
-  **Use common sense.** Remain suspicious. Treat all requests for confidential information or money with skepticism.
-  **Trust your instincts.** If a situation raises any doubts about authenticity, assume something is wrong.
-  **Always follow policy.** Security policies help protect the data of our employees, customers, and business partners.
-  **Report incidents immediately.** Big or small, all security incidents must be reported immediately to help mitigate damages.
-  **Ask for help.** There are no bad questions when it comes to security and privacy. Need more information? Please ask!

The Value of Personal Data

A common thread that connects almost all compliance laws is the protection of personal data. While each regulation has slightly different definitions for personal data, it's best summarized as simply "any information that identifies specific individuals."

That information carries a lot of value. But why do cybercriminals want it so much that they're willing to break laws in order to acquire it? Here are four common reasons:



Quick Profits

Put yourself in the shoes of a criminal hacker. You just exploited a security vulnerability and now have access to personal data of 100,000 people. What do you do with it? Perhaps the easiest option is selling it to other cybercriminals on the dark web—a small sector of the internet that often hosts illegal activity. The more data you have for sale, the more money you can make, especially if it's highly confidential information such as national ID or social security numbers.



Account Hijacking

Imagine the damage someone could do if they managed to gain access to a CEO's email account or a public official's social media handle. When usernames and passwords get stolen, it allows hostile individuals to take over accounts and lock out the authorized owners. In some cases, account hijacking is a mere nuisance. In extreme cases, it could lead to major financial consequences or jeopardize public safety.



Identity Theft

Identity theft represents one of the most threatening impacts of personal data being leaked or stolen. When someone gets ahold of your full name, address, phone number, date of birth, and national ID number, they can open fraudulent accounts in your name or file fake insurance claims. It often takes years for victims of identity theft to regain control of their identity and reestablish credit ratings.



Phishing Campaigns

Many generic phishing attacks are the result of contact directories getting leaked online. The scammers create a generic message and send a blanket email to everyone on the list. These types of attacks are usually easy to spot. But when phishers have access to enough data (beyond just email addresses), they can personalize phishing emails that target specific people. This is known as spear phishing, and it's one of the most effective cyberattacks around.

These reasons (and others) illustrate the importance of ensuring that confidential data remains confidential. As a reminder, you are the last line of defense. It's your job to know what kind of data you handle, know how to protect it, and to understand and follow current security policies.