What is Data Privacy and Why Should You Care?

Data Privacy Week is January 27 – 31, 2025!

What comes to mind when you think about privacy? Shutting the door for a private conversation? Locking your phone? Closing your window blinds? Since most of us are constantly connected to the internet nowadays, privacy includes how information about us and our families is used and shared. You deserve the right to control your data. This is the heart of data privacy—an essential issue now more than ever.

So, what exactly is data privacy, and why should it matter to you?

WHAT IS DATA PRIVACY?

We believe that privacy is a right. At its core, privacy is the fundamental right to control access to your personal life and information. This includes the right to keep certain information unseen or undisturbed by others.

From the vantage point of the 2020s, you're probably aware that the concept of privacy has evolved significantly. Let's work together to protect our digital spaces, which include your online identity, browsing habits, and even the messages you send. The right to privacy in this context means safeguarding your information from unwanted or unnecessary access.

UNDERSTANDING YOUR DATA

Data privacy centers on the right to protect personal information online. The sheer volume of data generated daily—from names and birthdates to medical records and browsing habits—is staggering. Even though so much is created, this data is highly valued by businesses and advertisers.

Types of personal data

Your personal data includes identifiable information such as your name, address, phone number, date of birth, and Social Security number. It also includes data about your behavior online, like the websites you visit, the products you buy, and even how long you stay on a webpage. Spending a few minutes streaming a video, perusing a webpage, or playing around on an app creates thousands to millions of data points.

Data is big business

Advertisers and other companies, such as so-called data brokers, prize this information. They collect it to create tailored ads, track purchasing trends, and study behavior. Often, companies "anonymize" data before selling it, but this anonymization doesn't entirely remove the privacy risk.

Data privacy vs. cybersecurity

While data privacy focuses on who has access to your data, cybersecurity is about protecting that data from hacking, malware, and other online threats. They work hand-in-hand, as secure systems help keep your data private, but we must stay informed and make intelligent privacy choices.

WHY IS DATA PRIVACY IMPORTANT?

You may wonder why data privacy matters if "everything is already online." But imagine this: you search for a product, and suddenly ads for it appear everywhere. Or perhaps you've downloaded an app that demands access to your contacts or emails, which it then sells to advertisers.

Here's why data privacy matters:

- Security: With more data shared online, the risk of unauthorized access increases. Protecting sensitive information like health records or financial details reduces the chance of them being misused.
- Choice: Being aware of data privacy allows you to make informed choices about what to share. Many apps or websites might request access to data they don't truly need—understanding your rights means you can decide what data you're comfortable sharing.
- Balancing privacy and convenience: Data privacy often involves trade-offs. For example, a maps app needs location data to provide directions. Knowing how to balance these choices helps you manage what data you disclose.

You have a say in your data privacy

Now that you understand why data privacy is essential, here are some practical steps you can take to protect your privacy in 2025!

1. Know what you can't control

Some data sharing is unavoidable. For instance, the IRS needs your income details. Similarly, many services, like navigation apps, require some data to function. Understand these limits so you can focus on what you can control.

2. Cultivate a data privacy habit

When apps or websites request access, ask yourself: Why does this app need this information? Simple games may ask for location data, which is likely unnecessary. Fortunately, many devices let you choose whether to grant data access. Think carefully before clicking "Allow" on any data request and deny permissions that don't make sense.

3. Check your settings regularly

Even if an app doesn't directly ask for data, it may still collect it. Periodically checking your privacy settings (monthly is a good habit) helps ensure your data-sharing preferences align with your comfort level. Here are a few tips:

- Turn off permissions like location, camera, or microphone access unless needed.
- Limit apps to access certain data only "while using" rather than "always."

Use Data Privacy Week 2025 as a nudge to check your settings right now!

4. Perform an app audit

Apps can collect data even if you aren't actively using them. Every few months, review your apps and delete any you haven't used recently. This simple step prevents unnecessary data collection and reduces clutter on your device. If you ever need the app again, you can easily reinstall it!

Write your own data story

While you can't always control how your data is shared, you can stand up for your data. Advertisers and tech companies think your data is valuable, and so should you! When you think of data as currency, these data privacy best practices empower you to control what you share and with whom. Making informed choices gives you peace of mind and a sense of agency in your digital life.

Remember, data privacy is your right. Celebrate Data Privacy Week 2025 by sharing this guide with others so they can take control of their digital presence.