

Why You Should Care About Data Privacy Regulations

Author : Cat

Date : October 29, 2019

I get it, Data Privacy Regulations are a pain. They are complicated and difficult to understand. Most of them are written in legalese. And, as a company, they take time and money to implement properly. But hear me out on this one... it will save you money in the long run to become compliant.

In the past businesses were able to put innovation ahead of individual rights and privacy. With the introduction of [GDPR \(General Data Protection Regulation\)](#) in 2018 for the European Union, we saw those priorities change. GDPR affects companies operating in the EU both physically and virtually. It puts user rights and data privacy at the forefront of how a business collects, stores, processes, and retains data. Other regions have implemented, or are establishing, their own versions of privacy regulations including PIPEDA (Canada), LGPD (Brazil), CCPA (California) and HIPAA (Medical Data).

When you look at these regulations from the perspective as an individual, this gives you back control of your personal data, which is an asset. You already decide what data you type in to a system but now you can also get insight on what data is being taken from you in terms of usage (location, connections, links you click on). You can opt out if the 'price' you pay in personal data is too high. This also protects your sensitive data such as medical, financial, and personal information.

As a company this seems like more work than it's worth. But there is actually tremendous value in following data regulations. Here are some of the risks you can mitigate and the benefits to becoming regulation compliant.

Corporate B2C - Business to Consumer

The business that deals directly with the consumer gets to decide what data is collected and how it will be used. In GDPR terms they are called Data Controller. By designing their service and/or product with privacy first thinking, the business can ensure that personal data is limited and protected.

BENEFITS OF COMPLIANCE:

- Following Privacy by Design and Privacy Engineering principles in the core of compliance will **significantly reduce the risk of breaches** because the personal data is limited and better protected. The ultimate goal of cybersecurity.
- Setting up processes to handle user data requests will **avoid stress on your system/company** under high load.
- When (not if) you are breached, compliance will **minimize fines from authorities and financial loss** from lost business.
- Having a pre-established Incident Response Plan (part of regulations) **saves you costs upwards up half a million dollars** when crisis hits.
- **Builds confidence with your consumer base** that you are trusted entity that complies with the law.

Corporate B2B - Business to Business

In the world of information, a business can act in the interest of a second business by storing, processing, or handling their data. In GDPR terms they are called Data Processor. In order to be compliant with most regulations, a company's third party processors, or vendors must also be compliant.

BENEFITS OF COMPLIANCE:

- Same rules as the controller company, following Privacy by Design and Privacy Engineering principles in the core of compliance will **significantly reduce the risk of breaches** because the personal data is limited and better protected.
- **Allows you to do business with global companies.** If your company is not compliant, your current customers in regulated regions will be forced to find other vendor companies that are.

Wondering where to start?

As a consumer, read up on the privacy policies you sign-in to and ensure your rights as an individual are being respected.

As a company, download our free [Global Data Regulation Compliance Overview](#) page to get an idea of what is included in the regulations and what areas you need to address to become compliant. Feel free to [reach out](#) at any point for more help.