From Europe to the United States – GDPR's Influence on American Privacy Laws

If you've visited a website in the past few years, you've likely encountered some type of pop-up message informing you of how that business handles your data, or a prompt asking you to manage your cookie preferences. Though this messaging is now commonplace, this wasn't always the case. These are just some of the ways we've all felt the impact of the European Union's General Data Protection Regulation (GDPR).

When the GDPR was adopted in 2016, it made headlines globally. This is because it set a legal precedent with high standards for the data privacy protection of individuals residing within EU member states. In fact, it's often considered the most stringent data privacy and security law in the world. Its influence has had a global impact, with noncompliant entities having to pay hefty fines. And legislative bodies in other countries are paying attention and following suit by enacting similar laws, including here in the United States.

As a business owner today, you must navigate a multifaceted data economy shaped by a complex regulatory landscape that dictates how you need to collect, store, and use customer data. We've recently discussed organizations' obligations with the Federal Trade Commission's renewed focus on cybersecurity and data privacy standards. **Now, let's highlight your responsibilities under the GDPR.**

THE GDPR'S CORE TENETS

At the heart of the GDPR is the principle that individuals have a right to own and control their personal data, and as such, it's up to them to decide who can use it. With the GDPR, the EU also intended to simplify the regulatory environment for businesses. The assumption was that it would be easier for organizations to adhere to one unifying, identical data protection law for a single market, though many companies have struggled to meet all of the GDPR's requirements.

Under the GDPR, data parties fall into 3 categories: data subjects, controllers, and processors.

1. **A data subject** is someone whose information is being gathered.
2. **A data controller** is an entity that processes the personal data of a data subject and must determine the purposes, circumstances, methods, and situations for processing this data.
3. **A data processor** is an organization that handles personal data on behalf of the controller.

Controllers and processors can be situated anywhere in the world, including the United States. Additionally, the GDPR only protects personal information that can be used to identify an individual, such as IP addresses, identification numbers, browsing cookies, email addresses, and more.

Some of the most important requirements businesses need to follow are:

- Obtain explicit consent for collecting data and deleting data if individuals withdraw their consent.
- Provide data subjects access to their information and implementing corrections and deletions, as requested.
- Allow individuals to take their data out of one system and put into another.
- Build business applications and processes with explicit measures to ensure data privacy and confidentiality.
- Be transparent with data subjects about who you are and why and how you're processing their personal data.
- Communicate with data subjects if you intend to use the data you've collected for a new purpose and reobtain their consent.
- Collect the smallest amount of data possible to complete the purpose you've communicated to data subjects.
- Justify the length of time you keep each piece of data you store, and anonymize it if you're not actively using it.

WHY SHOULD YOU CARE ABOUT IT?

Because GDPR applies to all people residing in EU member states, all businesses that operate within the EU must be GDPR-compliant. Yes, this also applies to organizations that don't primarily operate in the EU but have a user base in the EU.

> *For example, a social media or ecommerce business based in the United States that provides services to people in France would need to comply with GDPR.*

Though there is no equivalent to the GDPR at the Federal level, the tide continues to turn for the data privacy regulatory landscape in the US as existing laws are amended and new ones come into effect. With 80% of voters in the US supporting provisions to strengthen data privacy, expect these changes to continue in the years to come. Recently, several states have introduced or enacted legislation that follow the GDPR's footsteps.

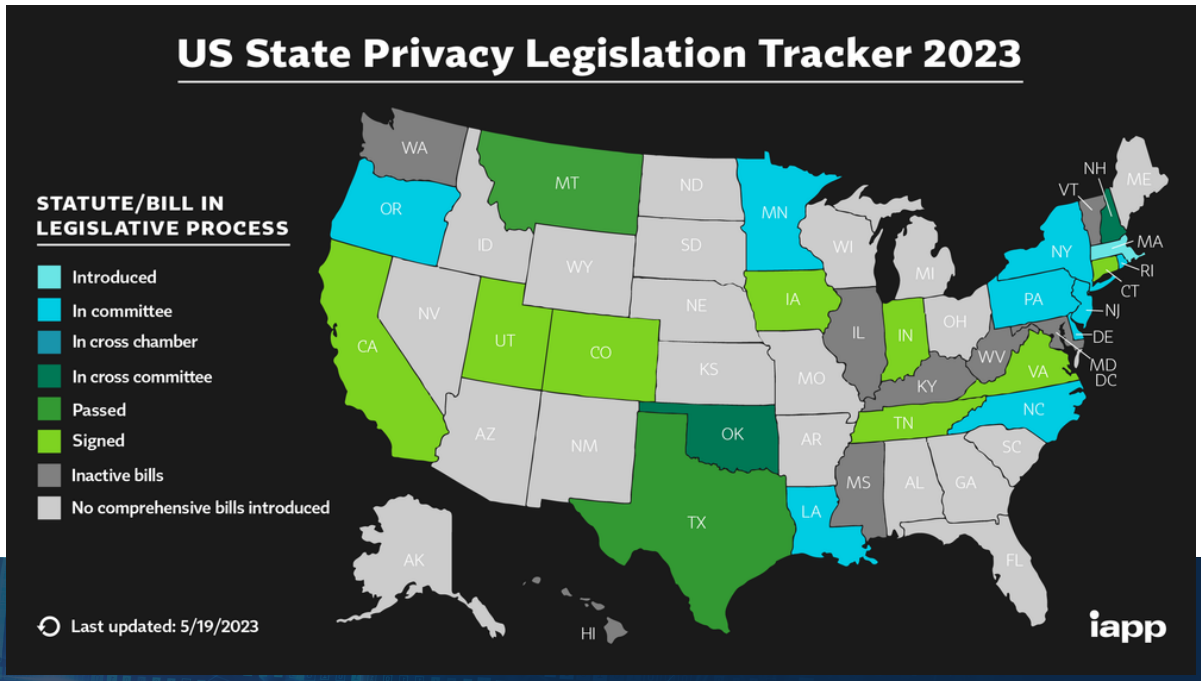

Image Source

Regardless of the laws your business needs to follow regarding data privacy, compliance with these rules and regulations can help you avoid costly fines and legal fees while maintaining customer trust and protecting your business' reputation.

STAYING ABREAST OF REGULATORY RISK

With many forms of technology not being geographically bound, the laws surrounding data storage and privacy can become hazy, quickly. **Be sure to review your data protection policies and technology with your legal team, IT department, executives, insurance advisor, and any other relevant parties** to ensure they're compliant with the GDPR, in addition to state and Federal level regulations. Try to stay informed about cybersecurity regulations so that you don't suffer the consequences should you be in the dark.

With regulatory scrutiny increasing both domestically and abroad, now is the time for a thorough review of your cyber policy with your insurance advisor. Should you be the subject of a regulatory investigation, you'll want to be sure that your cyber policy will provide an adequate level of financial protection for your business. Our team of cyber experts can help you find cyber coverage, explain what exactly your policy covers, and provide resources to help you be cyber secure and compliant.

You don't have to navigate the complexities of cyber risk alone. Connect with us to learn how we can help.

CONTACT US

AHT INSURANCE
A BALDWIN RISK PARTNER