GDPR in the USA: Compliance & Enforcement Guidelines | Matrix Point

https://www.thematrixpoint.com/how-gdpr-applies-in-usa

How does the GDPR apply to your business in the United States? MatrixPoint explains how to protect your business by ensuring it's fully GDPR compliant.

How the General Data Protection Regulation (GDPR) Applies to Your Business

The General Data Protection Regulation, or GDPR, is a regulation of EU law pertaining to privacy and data protection in the European Union and greater European Economic Area, while also addressing the transfer of personal data outside of these areas. While appearing to have a narrow scope of influence, the GDPR's reach extends far beyond just the EU and EEA. Businesses based in the United States with no EU operations may still be subject to enforcement and compliance for any traffic or users coming from these areas.

What Is GDPR?

The GDPR is a regulation that aims to give individuals more control over their personal data, while also simplifying the international regulatory environment by unifying the regulation under EU law. The regulation contains provisions related to the processing of personal data of individuals who reside in the EEA and applies to any enterprise that processes personal information of those residing in the EEA. This regulation applies even if the enterprise is not based in the EU or has any direct EU operations.

Compliance With GDPR in America

Compliance with the GDPR is compulsory for any business that collects personal information on anyone residing in the EU or greater EEA. This data can range from the simple collection of IP addresses from those visiting your website or network, to the collection of more specific and identifying personal information such as names and email addresses. Being extra-territorial in scope, this regulation even applies to companies outside of these areas that have no direct operations within these regions.

GDPR United States Enforcement

Article 50 of the GDPR outlines the guidelines for cooperation and enforcement of the regulation among the larger international community. In Europe, enforcement is led by numerous

supervisory authorities throughout the EEA. Internationally, mutual assistance treaties and other mechanisms are used to get local regulators to force violators into compliance and to levy any fines or additional punishments if necessary. US-based organizations have been collectively fined over $400 million dollars for various violations of the GDPR since 2018.

GDPR US Companies Applicability

The GDPR applies to any US company that collects any personal data of anyone in the EU, regardless if that business has any direct operations in the EU or greater EEA. As mentioned, this personal data can range from metadata such as IP and MAC addresses to more personally identifiable information such as contact information and even biometrics.

The GDPR utilizes the term "data subject" as reference to the individual whose data is being collected. Based on most interpretations of the law, the applicability of the GDPR is based on where the data subject is located at the time of collection and isn't necessarily tied to any citizenship or nationality. This means that generally speaking, the GDPR would apply to a US citizen who is in the EU at the time of collection, but not an EU citizen that is in the US.

GDPR Compliance US: What Does My Business Need To Do?

Any company based in the United States that collects or processes any personal information on users living in the EEA are subject to the GDPR. They are expected to comply with the same strict requirements that EU companies are in regard to the data protection and privacy of its users.

Organizations subject to the GDPR must also inform customers on why their data is being processed, and are required to provide transparent information about collection activities to data subjects. Consent is one of the six legal bases used to justify the collection and processing of user's personal data. Companies that process data based on consent are given more flexibility in regards to what they can do with that data, but are subject to additional standards and requirements. Your organization may need to update its privacy policy to ensure full transparency and compliance.

One of the landmark attributes of the GDPR is the new rights and controls given to individuals over their personal data collected by private companies. The GDPR introduces two key provisions in this regard: the right to erasure, and the right to portability of their data. Those rights include the right to access a copy of the data collected, the right to rectification, the restriction of processing, and even the right to object to processing, including automated profiling. Companies subject to the GDPR are expected to fulfill such requests and should be prepared to process them in a timely fashion to ensure compliance.

Companies should conduct a data protection impact assessment to help them better understand the security and privacy risks of the data being processed and to develop ways to properly mitigate them. The GDPR compliance checklist recommends the implementation of data security practices, such as implementing organizational safeguards and end-to-end encryption, to help limit your organization's and customer's potential exposure to data breaches. New projects developed to comply with the GDPR in USA should adhere to the principles of "data protection by design and by default."

Implement a data processing agreement with third-party clients to help further mitigate any risk. As the data controller, you will be held partially accountable for any GDPR violations your vendors may receive. This includes your email or cloud-storage provider, or any subcontractor that handles personal data. Implementing a data processing agreement that establishes the rights and responsibilities of each party is an effective and GDPR-compliant way to protect all parties involved.

Companies should review and update their internal processes and procedures to detect, investigate, and report any potential data breaches. If a data breach does occur, the data controller has no more than 72 hours to disclose the breach to the proper supervisory authority. If the breach poses a high privacy risk or a high risk to the rights and freedoms of the data subjects, then they too must be notified by the data controller or company. The EU recommends the use of strong encryption to mitigate exposure to fines and reduce your notification obligations should a breach occur.

For larger organizations, it may be necessary to designate a data protection officer. The data protection officer, or DPO, is a management-level employee tasked with overseeing an organization's compliance with the GDPR. The DPO is ultimately responsible for protecting users, ensuring GDPR compliance, and working with regulators if necessary. Employees in this position must have expert knowledge of data protection law and practices. In some cases, certain non-EU organizations are required to appoint a representative based in an EU member state. Article 27 and Recital 80 provide more specific details about which organizations this additional requirement applies to.

GDPR Fines for US Companies

With the GDPR comes significant enforcement powers meant to ensure proper compliance. Fines for violations can reach €20 million euros or up to 4% of an organization's worldwide annual revenue, per violation, whichever is higher. Data from the US International Trade Commission shows that since May 2018, EU member state data regulators have collectively imposed more than $417 million dollars in total fines against US companies under the GDPR. Under Article 50, the GDPR relies on mutual assistance treaties and other mechanisms to ensure international compliance and that violators are held accountable.

Contact MatrixPoint for Assistance

MatrixPoint is a specialty consulting firm dedicated to helping its clients navigate the complexities of the modern digital landscape. Our data privacy and compliance experts are ready to help ensure that your organization is fully GDPR compliant. Our team is able to assist with evolving regulations, help you expect the unexpected, rapidly adapt to disruption, and help you avoid any costly penalties and reputation damage associated with violations. Schedule a consultation today to learn more about MatrixPoint's data privacy management solutions and how they can benefit your organization.