What US Businesses and Individuals Need to Know About GDPR Compliance

The General Data Protection Regulation (GDPR) took effect in 2018, increasing data protection for European Economic Area (EEA) citizens and residents. The GDPR impacts how organizations collect, process, store, and share personal data. While the law applies to individuals in the EEA, GDPR compliance also affects American citizens and businesses in certain situations.

Failure to comply with GDPR can result in hefty fines, as well as reputational damage and legal action. For instance, Facebook's parent company Meta was fined $1.3 billion this year for violating GDPR guidelines. Companies need to understand whether they fall under GDPR and how to achieve compliance.

Additionally, American citizens fall under GDPR protection while living or traveling in a country protected by GDPR. For instance, an American vacationing in France has the same rights and protections as any other data subject in the EEA. Keep in mind that the EEA includes all European Union countries, plus Iceland, Liechtenstein, and Norway.

What Businesses Fall Under the Scope of GDPR?

In addition to European businesses, the GDPR applies to any organization outside the EEA that offers goods or services to EEA customers. It also applies to organizations that monitor the behavior of EEA users. Thus, GDPR may apply even if a business does not have a physical presence or target market in the EEA.

According to Article 3 of the GDPR, organizations must comply with the regulation if they meet either of the following criteria:

1. **They offer goods or services to EEA customers, even if they do not charge for them** – This means businesses need to consider not only their direct customers, but also potential customers who access their website or app. Examples might include an online store that ships goods worldwide or a blog providing advice to EEA readers.

2. **They monitor the behavior of EEA users** – This applies to organizations that collect, use, or analyze personal data about EU users. Personal data refers to data such as name, email address, IP address, location, or preferences. For example, businesses that use cookies or analytics tools on their website likely fall under this category.

Keep in mind that the GDPR has an "extra-territorial effect," meaning it applies to any organization that processes personal data of EEA individuals, regardless of their location. That is, a British citizen living in the U.S. still falls under GDPR protection.

Requirements for GDPR Compliance

The GDPR includes several key principles that govern compliance. The first involves transparency. Organizations must provide clear and concise information to individuals about how they process their data and for what purposes. This information should be displayed in easily accessible and understandable privacy notices or policies.

Another important principle involves consent. This means that organizations must obtain explicit permission from individuals before processing their data for specific purposes. Individuals may provide this permission via a clear statement or action, such as ticking a box or clicking a button. Additionally, individuals must have the ability to withdraw consent at any time.

When individuals have given consent for businesses to process their data, they retain certain rights related to that data. These rights include:

- Right to access – Individuals have the right to access their data and receive information about how it is being processed.
- Right to rectification – Individuals have the right to request the correction of any inaccurate or incomplete data concerning them.
- Right to erasure – Individuals have the right to request organizations to delete their data.
- Right to restriction – Individuals have the right to request that organizations limit data processing when they contest the accuracy of their data.

Finally, the GDPR introduces the principle of accountability. Under this requirement, organizations must demonstrate compliance. This involves implementing appropriate technical and organizational measures to ensure data protection. It also involves maintaining documentation of data processes activities such as data transfers and retention periods.

Data Governance Best Practices Aid GDPR Compliance

Complying with the GDPR and similar privacy regulations in the U.S. can prove challenging. Implementing data governance strategies can help. For instance, businesses might start by conducting a data inventory to identify the personal data they process and what happens to it.

Businesses should also update their security and privacy policies on a regular basis to ensure data protection and transparency. And they should implement or revise consent mechanisms to make sure they obtain valid consent from data subjects. Finally, security and compliance monitoring will alert the organization to potential issues early on.

The data governance experts at Messaging Architects offer a range of GDPR services to help organizations achieve compliance. Additionally, our consultants can assist with designing and implementing solid data governance strategies to ease future compliance efforts.