The Risks of GDPR Non-Compliance

In 2016, the European Union (EU) adopted the General Data Protection Regulation (GDPR). This legislation strengthens rules on data protection to allow individuals greater control over their personal data. The GDPR rules take effect on May 25, 2018, after which supervisory authorities may impose a range of penalties for GDPR non-compliance.

The GDPR applies to companies, government agencies, non-profits, and other organizations that do business with people in the EU, or that collect and analyze data tied to EU residents. The GDPR applies no matter where the organization is located.

Despite ample warning, a significant percentage of businesses in the United States have yet to establish GDPR compliance. With the deadline upon us, it is important to understand the risks of non-compliance. The legislation itself outlines penalties that could severely impact the bottom line. Other related consequences could prove even more damaging.

Tiered Penalty Structure

Violations of basic principles of the GDPR can result in fines of up to four percent of annual global revenue. While such a fine could prove devastating, particularly to a small business, there are actually two tiers of penalties. In addition, fines represent just one of several possible sanctions.

Supervising authorities will consider several factors when determining fines or other consequences. These factors may include the nature of the violation, the types of personal data affected, intent or negligence and the degree of cooperation with authorities. Once imposed, fines fall into one of two tiers:

- Lower Tier – In general, these involve failing to adequately integrate data protection by design into business operations. Fines can be imposed of up to 10 million euros or two percent of the organization's annual global revenue, whichever is greater.
- Higher Tier – These involve more serious infringements on an individual's privacy rights and freedoms. Fines in this category can reach as high as 20 million euros or four percent of annual global revenue.

Additional Consequences of GDPR Non-Compliance

Although severe fines gain the most attention, other consequences of GDPR non-compliance can prove at least as harmful. Consider these additional possible repercussions:

- Damage to Reputation – When consumers learn that your organization has had an incident, they will be wary about trusting you with their data. Even a formal reprimand can result in loss of market share and reduced consumer confidence.
- Cost of Damage Control – Once an incident has occurred, it will be costly to conduct investigations and implement remediation measures.
- Withdrawal of Certification – Supervisory authorities can mandate withdrawal of a certification.

- Ban on Processing – Supervisory authorities may also order a temporary or definitive ban to keep your organization from processing personal data.
- Liability for Damages – According to Article 82 of the GDPR, an individual who has suffered material or non-material damage as a result of an infringement of the GDPR can claim compensation from both data controllers and data processors.

Small Business and GDPR Non-Compliance

The GDPR is implemented using a risk-based approach. That means the more data you process, the more the rules apply to your organization. This is good news for most small to medium businesses (SMBs), as large fines could be disastrous for small firms.

For instance, if you employ less than 250 people, and processing personal data is not part of your core business, you probably do not need to appoint a Data Protection Officer. In addition, the requirement to keep records of processing activity is less stringent if processing of personal data does not pose a threat to the rights and freedoms of individuals.

Mitigating the Risk of GDPR Non-Compliance

Regardless of the size of your organization, take the time to bring your business into GDPR compliance and to maintain compliance moving forward. The more transparent the processing of personal data, the better.

Some businesses may not be able to comply with every aspect of GDPR by May 25. If so, be ready to demonstrate that you are making a good faith effort to come into compliance. Know where your data comes from and how you store it. Understand the GDPR rules for consent and begin to implement them.

While the principles of GDPR can seem overwhelming, help is available. Whether implementing cloud solutions with built-in, audit-ready tools or performing a GDPR readiness assessment, data compliance experts stand ready to assist.