cioxchange

Driven by CIOs, fueled by Gartner

Driving Business Transformation: Leadership in a Digital World

Top 5 Priorities to Prepare for EU GDPR

50 percent of organizations will fail to comply with GDPR.

When the European General Data Protection Regulation (GDPR) comes into effect on May 25, 2018, its impact will extend beyond the borders of the European Union (EU). It will apply to all companies processing and holding the personal data of EU residents, regardless of the company's location.

"The GDPR will affect not only EU-based organizations, but many data controllers and processors around the globe," said Bart Willemsen, research director at Gartner. "With the renewed focus on individual data subjects and the threat of fnies of up to €20 million or 4% of annual global turnover for breaching GDPR, organizations have little choice but to re-evaluate measures to safely process personal data."

Despite a lot of recent attention around these regulations, Gartner predicts that, on the date of effectuation, more than half of companies affected by the GDPR will not comply fully with its requirements.

Organizations must focus now on fvie high-priority changes to ensure compliance when GDPR comes into force:

1. **Determine Your Role Under the GDPR**
   Any organization that decides on why and how personal data is processed is essentially a "data controller." Therefore, the GDPR applies not only to businesses in the EU, but also to all organizations outside the EU that are processing personal data for the offering of goods and services to the EU, or that are monitoring the behavior of data subjects within the EU. These organizations should appoint a representative to act as a contact point for the data protection authority (DPA) and data subjects.

2. **Appoint a Data Protection Officer**
   Many organizations will be required to appoint a data protection offcier (DPO) as a result of the GDPR. This is especially important when the organization is a public body, is processing operations requiring regular and systematic monitoring, or has large-scale processing activities. "Large scale" does not necessarily mean hundreds of thousands of data subjects — early drafts of the GDPR mentioned the processing of data on more than 5,000 subjects in any 12-month period.

> *continued on next page*

cioxchange
Driven by CIOs, fueled by Gartner

> *continued from previous page*

3. Demonstrate Accountability in All Processing Activities
Purpose limitation, data quality and data relevance should be decided on when starting a new processing activity, but also applied to existing processing activities. This will help to maintain compliance in future personal data processing activities. Organizations must demonstrate accountability and transparency in all decisions regarding personal data processing activities."Third-party service providers (i.e. data processors) must also comply, and this will impact an organization's supply, change management and procurement processes," said Mr. Willemsen. "Accountability under the GDPR requires proper data subject consent acquisition and registration. Pre-checked boxes and implied consent will no longer be suffciient. Instead, organizations will be required to implement streamlined techniques to obtain and document consent and consent withdrawal."

4. Check Cross-Border Data Flows
Data transfers to any of the 28 EU member states will still be allowed, as well as to Norway, Liechtenstein and Iceland. Transfers to any of the other 11 countries the European Commission (EC) has deemed to have an "adequate" level of protection will also be possible. Outside of these areas, organizations should use appropriate safeguards, such as Binding Corporate Rules (BCRs) and standard contractual clauses (i.e., "EU Model Contracts").

5. Prepare for Data Subjects Exercising Their Rights
Data subjects have extended rights under the GDPR. These include the right to be forgotten, the right to data portability and the right to be informed (e.g., in case of a data breach, or to receive an explanation, for example in machine learning systems' automated decision making).

"If a business is not yet prepared to adequately handle data breach incidents and subjects exercising their rights, now is the time to start implementing additional controls," Mr. Willemsen said.

Connect

Twitter

LinkedIn

Facebook