Written by Marco Attard
05 May 2017

According to Gartner the European General Data Protection Regulation (GDPR) will have a global impact once it goes into effect on 25 May 2018-- and over 50% of companies will not comply with it.

"The GDPR will affect not only EU-based organisations, but many data controllers and processors outside the EU as well," the analyst states. "Threats of hefty fines, as well as the increasingly empowered position of individual data subjects tilt the business case for compliance and should cause decision makers to re-evaluate measures to safely process personal data."

The GDPR is a replacement of Data Protection Directive 95/46/EC. It is designed to support the single market, harmonise data privacy laws across Europe, and protect and empower the data privacy of EU citizens. As such, it reshapes the way organisations approach data privacy for EU citizens, wherever they work in the world.

Gartner suggests 5 high-priority for companies wanting to get to speed with GDPR requirements:

1. **Determine your role under the GDPR**-- An organisation processing personal data is a "data controller," and the GDPR applies to all organisations outside the EU processing personal data to offer goods and services to the EU, or monitoring the behaviour of data subjects within the EU. Such organisations need to appoint a representative acting as a contact point to the data protection authority (DPA) and data subjects.

2. **Appoint a Data Protection Officer (DPO)**-- This is especially important when an organisation is a public body, processing operations requiring regular and systematic monitoring, or has large-scale (not necessarily hundreds of thousands of data subjects) processing activities.

3. **Demonstrate accountability in all processing activities**-- Organisations must be accountable and transparent in all decisions regarding personal data processing, and outside parties must comply with relevant requirements impacting supply, change management and procurement processes. The GDPR demands proper data subject consent acquisition and registration, with prechecked boxes and implied consent largely a thing of the past.

4. **Check cross-border data flows**-- Data transfers to any of the 28 EU member states are still allowed, as well as to Norway, Liechtenstein and Icelend. Transfer to the other 11 countries in the European Commission (EC) having an "adequate" level of protection are also possible. Outside these areas, appropriate safeguards such as Binding Corporate Rules (BCRs) and standard contractual clauses (EU "Model Contracts") should be used. EU-based data controllers should pay attention to new mechanisms under the GDPR when selecting or evaluating data processors outside the EU and ensure appropriate controls are in place. Outside of the EU, organisations processing personal data on EU residents should select appropriate mechanisms to ensure GDPR compliance.
5. **Prepare for data subjects exercising their rights**-- Data subjects have extended rights under the GDPR, including the right to be forgotten, to data portability and to be informed in case of data breach. This means businesses need to start implementing additional controls.

Gartner also points out entities subject to legislation should seek further legal counsel from qualified sources. There's also the matter of Brexit, which is unsure as yet, since the UK might receive a positive adequacy decision by the EC or become a European Economic Area (EEA) member.

Go Gartner: Focus on Five High-Priority Changes to Tackle the EU GDPR