GDPR compliance: what organisations need to know

information-age.com /gdpr-compliance-organisations-need-know-123465756/

18 April 2017

The EU General Data Protection Regulation represents one of the biggest change to data protection laws, and businesses must be prepared

Since data protection regulations will be the same throughout Europe, organisations no longer need to consult local lawyers to ensure local compliance, which results in direct cost savings and legal certainty

The new EU General Data Protection Regulation (GDPR) in Europe, adopted in 2016, will be directly applicable starting on May 25, 2018. GDPR comes with significant changes compared to the Data Protection Directive 95/46/EC involving operational changes in organisations.

As a result, organisations need to be extremely aware of these changes as they can face very strict fines in the cases of non-compliance.

The most important change in data privacy regulation in 20 years, GDPR is a regulation issued by the European Commission, the European Parliament and the Council of Ministers of the European Union with the goal of improving data protection for individuals within the European Union.

With this regulation, the EU aims to give its citizens more control over how their personal data is used as well as provide businesses with a clearer legal structure with which to operate by standardising across the EU.

Who is impacted?

The GDPR applies to controllers and processors that are handling the personal data of European individuals. Perhaps one of the most important things to note is that this new regulation applies to ALL organisations

collecting and processing personal data of individuals residing in the EU, regardless of the company's physical location.

Article 4 of the EU GDPR clarifies the different roles between controllers vs. processors, which are defined as:

Controller – "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".

Processor – "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

In short, a data controller specifies how and why personal data is processed, while a processor conducts the actual processing of the data. The controller is responsible for ensuring their processor abides by data protection law.

However, processors also must follow the regulations and maintain records of their processing activities. With the new regulations, if processors are involved in a data breach, they are far more liable than under the previous Data Protection Act.

What does the new GDPR entail? How to be compliant

Extended jurisdiction – Regulations will apply to any company collecting and/or processing EU citizen's personal data regardless of where the company's physical offices are located.

Consent – Organisations will be required to obtain individual's consent to store and use their data as well as explain how it is used.

Mandatory breach notification – Organisations will now be required to notify the supervisory authority within 72 hours of discovering a security breach unless it is unlikely to "result in a risk to the rights and freedom of individuals."

Right to access – Companies must be able to provide electronic copies of private records to individuals requesting what personal data the organization is processing, where their data is stored and for what purpose.

Right to be forgotten – EU citizens will be able to request the controller to not only delete their personal data but to stop sharing it with third parties – who are then also obligated to stop processing it.

Data portability – The new regulation gives individuals the right to transmit their data from one controller to another. As a result, upon request, organizations must be able to provide an individual's personal data in a 'commonly used and machine readable format.'

Privacy by design – This will be a real game-changer. Privacy by design is now a legal requirement in GDPR. This means that security must be built into products and processes from day one.

Data protection officers (DPO) – Both data controllers and data processors are now required to appoint a DPO – who can either be a contractor, new hire or a member of the organisation's staff.

It is important to note that not all companies are obliged to have a DPO. Only those "whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences."

Consequences of non-compliance

At the end of 2016, a survey conducted by AvePoint on 223 respondents from multinational organisations revealed that only 26% kept records of data processing and transfers. This is worrying as the penalties for non-compliance are significant.

The penalties are separated in two tiers and vary depending on many factors including – among others – the

duration of the infringement, the number of the data subjects affected and the level of impact.

For more severe non-compliance, organisations can be fined either up to 20 million euros or four percent of the total worldwide annual turnover of the preceding financial year, whichever is higher.

For less severe breaches, organisations can face fines of either up to 10 million euros or two percent of the total worldwide annual turnover of the preceding financial year.

How can compliance cut costs?

While getting to full compliance can be difficult and complicated, once full compliance is achieved, organisations will likely see significant benefits – especially for larger corporations looking to enter new markets.

Since data protection regulations will be the same throughout Europe, organisations no longer need to consult local lawyers to ensure local compliance, which results in direct cost savings and legal certainty.

If your organisation will be impacted by the new regulation, your next step is to identify what data you store and process for European citizens, its location, its path from point A to B, by what systems is it processed, etc.

By doing this, you can understand if your organisation has the required tools to protect private data, or it will shed insight onto the tools you may need to support your organisation in achieving GDPR compliance.

Conducting an audit and investing in solutions like data loss prevention can help get you to compliance faster. Treat compliance with GDPR as a project and get a lawyer to ensure you adhere to all guidelines.

Sourced by Roman Foeckl, CEO, ***CoSoSys***