EU Data Protection Regulation 2017

brought
to you by Seefin
Data Management

What is...

the European Data Protection Regulation?

In January of this year the European Commission revealed a draft of its European Data Protection Regulation to replace the previous Data Protection Directive.

The Data Protection Directive is a European Union Directive, which was created to regulate the progression of personal data within the European Union. Officially known as the Directive 95/46/EC the legislation is part of the EU privacy and human rights law.

The aim of the new European Data Protection Regulation is to harmonise the current data protection laws in place across the EU member states. The fact that it is a "regulation" instead of a "directive" means it will be directly applicable to all EU member states without a need for national implementing legislation.

The first EU Data Protection Directive was written in 1995 but a new, stronger regulation is being developed to take into account vast technology changes of the last 20 years. The plan is to finalise the regulation this year and implement it in 2017.

As with any regulation, the current draft could change. However, only minor changes were made between the last two drafts, despite lobbying attempts, and the latest version is as close to final as we'll see.

Below are 10 of the most important elements organisations should take away from the proposed reform, to help them prepare for 2017:

1. This is a Regulation, Not a Directive

A 'directive' is implemented and enforced by individual countries but **'regulations' become law without change when they are passed**. The current EU data protection directive resembles a patchwork of slightly different laws across Europe but **the new regulation will be implemented in all 28 countries.**

2. Data Processors Responsible for Data Protection

Under the new regulations, any company or individual that processes data will also be held responsible for its protection, including third parties such as cloud providers. Put simply, **anyone who touches or has access to your data, wherever they are based, is responsible in the case of a data breach**. The ramifications of this are pretty broad. Third parties will need to be extra vigilant when it comes to securing the data of others, and data owners will want to thoroughly vet their partners.

With the new regulations in mind, **organisations should think about reviewing their third party contracts** now. In the case of cloud providers seriously consider having, as part of your contract, the ability to carefully review their procedures and even facilities to make sure they are up to scratch. Many cloud service providers, especially those based outside the EU, may not believe that the regulations apply to them, it is clear that they will.

3. The Regulation has Global Ramifications

Don't let the terms 'EU' or 'Europe' fool you, **the new regulation affects every global organisation that may have data on EU citizens and residents**. Reputational damage is also a key element of a data breach and the new regulation is likely to harmonise 'naming and shaming' policies across each country. For instance, in the UK, the Information Commissioner's Office issues press releases when organisations are sanctioned at the moment, whereas some other countries are more lenient.

4. Users Will Be Able to Make Compensation Claims

The regulation will allow users to claim damages in the instance of data loss as a result of unlawful processing, including collective redress, the equivalent of a US-style class action lawsuit. Senior management will need a good understanding of what kind of impact this would have on their business. **Not only can legal damages be incredibly costly from a financial perspective, they also represent further reputational damage as cases can carry on for years and keep the story in the public eye throughout this time**.

5. Harder to Export Data of EU Citizens

Even if sharing is allowed the directive currently prohibits personal data from being transferred outside the European Economic Area (EEA) unless the controller assures an adequate level of privacy protection. **When negotiating with a cloud provider, pose the question of whether they are allowed to move data between countries as part of the contract, whether they have to inform you of such a move or can only do so at your request.** Get visibility into the CSP's HQ and data storage facilities (don't assume it is the same) and also any countries where they employ people who manage the service. Furthermore, whereas the directive allows a data controller to decide if a third-party provider is safe, under the regulation, only the commission can do so.

6. Harmonised User Request Rights

Under the directive, users already have the right to see the data collected about them. However, each country currently defines how data controllers should respond and in the proposed regulation **the deadline will be harmonised to approximately 20 days.**

7. New Erasure Rights

In the new regulation, **users can demand that their data be erased**. This may sound straightforward but it's not always that simple. **If a person said they wanted to be removed from one of your databases, how would you go about doing so?** Would you have to remove data from multiple systems? Are syncing protocols in place that would make doing so difficult? Do you have processes now for this and how would you remove contact information from individual databases or spreadsheets? **These are questions that need answering now**, not after the regulation comes into play.

8. You Must Inform Users of their Rights

Under the new regulations, controllers must inform and remind users of their rights, as well as documenting the fact that they have reminded them of their rights. **In addition, users should not have to opt-out of their data being used, they must opt-in to your systems**. This is more stringent than the current directive and **companies that fall foul of these measures will face larger fines.**

9. Tougher Sanctions

This is the big one. In case there was any doubt about how serious the regulators are taking the data breach issue, sanctions have been made much, much tougher. **Fines may be as high as €100m or 5 percent of global revenue** (whichever is higher), in stark contrast to what we currently have here, which is a maximum fine of nearly €600,000.

10. Encryption/Tokenisation to the Rescue

It's not all bad news, there's a piece in the regulation saying that **controllers must meet individuals' "reasonable expectations" of data privacy**. This is an interesting term as the regulations stipulate that tokenised, encrypted or pseudo-anonymised data does indeed meet these expectations. This is great news, as it allows organisations to encrypt or tokenise data before uploading to the cloud. **Assuming that companies keep the encryption keys on their own premise, firstly data loss is much less likely and, if it does happen, they can show the regulators that they took steps to "meet the individual's reasonable expectations of data privacy".**

Conclusion

This period, when the regulation is drafted but not yet in effect, is the ideal time for IT, security, and compliance teams to review the new requirements, seek legal guidance and put into place the systems and processes that will enable compliance.

If you would like any further advice or information, why not arrange a free consultation with Seefin Data Management and make sure your data is in shape for the New Year?

Seefin
Data Management Ltd.

www.SeefinDM.com

info@SeefinDM.com

Office: +353 (087) 834 6670