WHITE PAPER

General Data Protection Regulations [GDPR] – what you need to know

"In the world of Data Protection Law, General Data Protection Regulation (GDPR) is considered a milestone achievement by the EU. Despite the advancement of the digital era, the EU Data Protection Law remained fairly static for nearly 20 years. However, after three years of detailed discussions, a political agreement led the European Commission, the EU Parliament and the Council of the EU to take a big step towards replacing Data Protection 95/46/EC with GDPR."

Summary

GDPR represents a unified data protection law for Europe's 500 million citizens. This law is expected to offer greater accountability and transparency by offering controls for individuals to efficiently manage their data.

The aim of establishing the GDPR is to bring one single set of rules that will make it simpler for companies to run their businesses in the EU. Therefore, implementation of these data protection regulations is necessary in the roll-out of new services and technology.

This white paper should be read in conjunction with Episode's **BS EN 10012 Personal Information System information sheet**. BS 10012 PIMS, has been specifically written to help you both comply with the law, and have independent validation of the effectiveness of your approach to GDPR.

Why Episode

Episode has built many ISO compliant systems. Our systems capture what you do and how you do it. We will only ask you to change how you do things, or do new things, if it is absolutely necessary.

We have helped organisations already certified to make ISO work for them, not the other way around. We have also worked closely with a certification body that independently certifies you against the Standard to design a simple and effective GDPR approach. .

As part of our approach, our cyber security partner, Bleam Cyber Security Limited provides specialist technical advice.

Episode will complete a review of your organisation and provide everything you need for successful certification within pre-defined timescales, for a fixed fee, and we guarantee success.

Episode consultants Ltd
95 Gateland Lane
Shadwell, Leeds LS17 8LW

0113 801 9001
info@episodeltd.com
www.episodeltd.com

episode
RAISING THE STANDARD

More detail

The GDPR has a far reaching consequences, since if a company wishes to conduct business with an organization that is European, it must abide by these regulations, irrespective of its position on the continent. This law would appear to have huge ramifications as it is set to apply to any e-commerce vendor whose target is to sell their products and services to European customers. Furthermore, according to the draft GDPR regulations, large businesses with more than 250 employees, along with those organizations that work on data processing operations, will be required to appoint dedicated data protection officers.

Another significant accomplishment for GDPR is with regards to the notification time. Organizations will need to notify the regulator about any breaches within 72 hours.

One of the major goals of GDPR is to ensure that organizations define their specific consent model as well as the processes that they use for capturing data. They also must ensure that individuals are able to retain control over their own data.

Furthermore, according to GDPR it is necessary that companies consider the requirement that any third parties which process information must also be proactively governed. This makes it easier for organizations to identify how and where information is processed, stored and transmitted. These regulations allow organizations to be clear about their actions while also protecting organizational structures, governance and technical requirements.

GDPR is certain to increase organizations' focus on securing their data and the skills that they must acquire to address the data security challenges. With its new requirements and penalties, GDPR will certainly prove itself to be a game-changer for data protection.

One of the many changes that the new Regulation will deliver when it comes into force on 25 May 2018 is a new statutory obligation on data security that data processors must observe above and beyond contractual duties agreed with data controller customers.

Under current EU data protection rules service providers that process personal data on behalf of other businesses cannot be held directly liable to individuals for a breach of data security. If data processors are at fault for data breaches then it is the data controller who contracted with them who is on the hook for any non-compliance with data protection laws, although the data processor could be liable to the data controller under their contract.

The Regulation addresses this anomaly but makes a distinction between the maximum fine data protection authorities will be able to levy against data controllers compared to data processors for failings on data security.

A two-tiered sanctions regime will apply. Breaches of some provisions by businesses, which law makers have deemed to be most important for data protection, could lead to fines of up to €20 million or 4% of global annual turnover for the preceding financial year, whichever is the greater, being levied by data watchdogs. For other breaches, the authorities could impose fines on companies of up to €10m or 2% of global annual turnover, whichever is greater.

The relevant provisions on data security are contained under Articles 5 and 32 of the Regulation. Article 5 sets out basic rules on personal data processing which only apply to data controllers, considered to be fundamental to data protection.

One of those rules requires data controllers to ensure that personal data is "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

According to the Article 83 provisions of the Regulation on administrative fines, where data controllers breach that Article 5 requirement they can be served with the highest possible fine that data protection authorities will be able to issue under the reformed framework.

In contrast if data processors breach their statutory data security obligations, set out under Article 32, which requires them to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk" of their personal data processing, then the most they could be fined is up to €10m or 2% of global annual turnover.

Data controllers are also subject to the Article 32 obligations. It therefore appears open to national data protection authorities to fine data controllers for any data security failings under Article 5 or Article 32. Their choice in those circumstances would impact on the severity of the fines they could issue.

Whether security measures are appropriate in each instance will depend on "the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons", according to the Regulation.

Beyond the imposition of administrative fines for data security breaches, the Regulation will also introduce an updated right for data subjects to claim compensation for damages they suffer from such incidents. A data controller or data processor could be sued for compensation as well as being exposed to the administrative fines – being fined will not shield it from compensation claims, and vice versa.

The revised right will allow data subjects to pursue either data controllers or data processors for all of the compensation owed to them for the damage they have suffered from a data breach, although a processor will only be liable for damage caused by processing where it has not complied with any part of the Regulation that applies to them or if it has "acted outside or contrary to lawful instructions of the controller".

Data controllers pursued for damages will be able to claim back all or some of the money they pay out from their data processor if the data processor was in fact responsible, wholly or in part, for the breach. Equally, data processors will have the same right to claim back money from data controllers, or indeed other data processors involved, whose fault caused or contributed to the damage, if the data subject pursues the data processor for the full compensation pay-out.

As a result of the changes, data processors and controllers will both want to negotiate the scope of their obligations, liabilities and indemnities accordingly.