GDPR Primer

Regulatory Update
February 2017

axxsys

GDPR – General Data Protection Regulation

An introduction to the European Data Protection Act

The European Commission has published a Regulation, see [REG], and a Directive, see [DIR], outlining the legal framework for protection of personal data inside the European Union. The Regulation entered into force on May 24th 2016 and is expected to apply from May 25th 2018. The Directive entered into force on May 5th 2016 and is expected to be transpose into national law by May 6th 2018. See [DP] for details.

What is the Data Protection Act All About?

The aim of the Regulation is partly to give citizens back control over personal data by requiring companies to process data lawfully, fairly and in a transparent manner in relation to the data subject, and partly to harmonise the protection across the EU. While the details of the Directive still remains to be worked out by National Authorities, it is clear from the Regulation that many companies will find themselves in a situation, where their entire data infrastructure and data model will need to be reconsidered and enhanced in order to comply with this Regulation.

The regulation sets an administrative fine of 4% of annual worldwide turnover or EUR20 million (whichever is highest), for some infringements, other specified infringements would attract a fine of 2% of turnover or EUR 10m. The EU GDPR framework is not unique in this field, although to date this is it is seen as the strictest framework in the world.

Who is impacted by this Regulation?

GDPR applies to processing carried out by firms operating within the EU, it also applies to firms outside the EU that offer goods or services to individuals in the EU, that as part of their business deal with individual's personal information (this includes customer and employee data), insurance companies and wealth managers are good examples.

What are the Likely Challenges Arising from the Regulation?

The problems which needs to be addressed are many and tedious by nature. First, it needs to be worked out exactly what quantify as 'personal data' across organisations. Second, it is unlikely that data holders have structured their data model such that 'personal data' has been tagged, and hence can be easily identified, and it is even more unlikely that records exists specifying exactly what purpose the data was originally collected for (and that the data subject has approved the manner it is being processed). Third, it needs to be verified if the data is being used in another context beyond the purpose it was originally collected for, and a decision needs to be made what to do, if this is the case. Forth, processing activities needs to be recorded and even if companies already do so, it is unlikely to satisfy the format dictated by the Regulation. Finally, it must be verified that the data access and security model is fit for purpose, and if not the IT policy must be updated accordingly.

Beyond the reputation risks associated with being caught non-compliant with this Regulation, companies holding personal data must further take into consideration that this Regulation gives data subjects the right and framework to complain and obtain redress, if personal data is found be have been misused anywhere within the EU.

GDPR includes provisions that promote accountability and governance, responsibility for data privacy has historically been left with IT, legal or compliance, however senior management awareness and engagement from the business and wider functions will be key is minimising the impact and spend of GDPR programmes and reaping benefits from improved data management practices.

Axxsys Consulting can help

Data Protection creates challenges, but it does offer an opportunity for firms to address digitisation as a broader topic, and adopt sophisticated techniques for data management and control.

A 'personal data' management structure needs to be put in place (or an existing structure must be enhanced) including a security framework such that access can be managed, controlled and granted. This structure must address both internal considerations and how data can safely be exported to external sources, if need be.

Axxsys Consulting has extensive experience in working on complex data models in environments where data generally are of a sensitive nature. Axxsys also have resources with deep knowledge of most vendor systems. We are therefore uniquely positioned to assists companies address regulatory challenges such as GDPR.

Axxsys have developed a GDPR Accelerator to help you become compliant as quickly and efficiently as possible.

The Axxsys GDPR Readiness Assessment program provides you with the guidelines and templates to kick start your GDPR plan and continuously assess your GDPR compliance level, and the tools and resources to achieve compliance ahead of the deadline.

For more details of our Complete GDPR Compliance solution here http://www.axxsysconsulting.com/factsheets.php

For more information about Axxsys' Personal Data Protection consulting services, please contact Klaus Krarup – kkrarup@axxsysconsulting.com

References

[DP] http://ec.europa.eu/justice/data-protection/

[REG] http://eur-lex.europa.eu/legal- content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

[DIR] http://eur-lex.europa.eu/legal- content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

GLOBAL OFFICE NETWORK

LONDON	COPENHAGEN	LUXEMBOURG	PARIS	AMSTERDAM	EDINBURGH
TORONTO	GENEVA	ZÜRICH	NEW YORK	BOSTON	SINGAPORE

www.axxsysconsulting.com
info@axxsysconsulting.com