AmberGate™

Privacy. Security. Compliance.

GDPR - An Introduction

Last updated 24 November 2017

The European General Data Protection Regulation 2016/679 ('GDPR') comes into force on 25 May 2018 and, as a regulation, will have direct effect throughout the EEA without any need for implementation by the UK and other Member States.

In brief

Many parts of the GDPR (which runs to 173 Recitals and 99 Articles) incorporate a risk-management approach, although there are major strict obligations that cannot be avoided. Existing obligations, not least on consent and using processors, will become far more demanding. Many new obligations on data controllers- and for the first time data processors - mean historical records and actions will need to be reviewed and refreshed, ongoing governance will need to be created, and data systems will need overhauling to address new data subject rights.

However, while the GDPR toughens and extends the current regulatory regime, those who are in a good position with data protection now are in a good position for their GDPR project. Those starting out need to move quickly but much can be achieved in a short period with the right senior sponsorship and corporate will.

The key is to take hold of the project and keep it moving forward it with an efficient, commercial and expert approach. There are many myths and misleading statements out there.

Increased Fines

You are probably aware that fines for infringement of the GDPR are greatly increased from current levels. **The maximum fine is now €20m or 4% of total worldwide annual turnover in the preceding financial year, whichever is greater**.

Without any doubt, this confirms data protection as a board-level matter. Directors as a whole, and Audit Committees in larger companies, will need to be sure that their business is in compliance and managing its risk.

As an example under the current, pre-GDPR regime with a maximum fine of £500,000, on 30 September 2016 the UK Information Commissioner ('UK ICO') fined Talk Talk Telecom Group PLC £400,000 for a breach in 2015 that led to the personal data of 156,959 customers being compromised, including bank account and sort code details for 15,656 customers[1]. And the fine was made **after** taking into account mitigating factors. The breach was down to a simple SQL injection attack on a legacy database vulnerability for which a patch had been available.

Hot on the heels of that huge fine, Talk Talk was again fined by the UK ICO on 7 August 2017 for £100,000, for a breach that led to the personal data of up to 21,000 customers being compromised[2]. Again the fine was set **after** taking into account mitigating factors. The breach was again down to poor security, in particular access control for a support portal in 2014 (before the SQL injection attack).

Both of these breaches were suffered due to poor information security on Talk Talk's behalf, addressable by common security practices, leading to Talk Talk being in breach of its obligation to implement appropriate technical and organisational measures to safeguard personal data. Both fines show that even the more pragmatic and commercial UK regulator is more than willing to make full use of monetary penalties.

Global reach

Many businesses with no establishment or equipment in the EEA will be subject to EU data protection law for the first time from 25 May 2018. The GDPR creates global reach for the EU's data protection laws and covers processors for the first time.

The GDPR applies to data controllers and processors with establishments in the EU. However, the GDPR also applies to those outside the EU:

- who process the personal data of EU residents to offer them goods or services or monitor their behaviour in the EU
- Who are otherwise subject to Member State law

Existing obligations increased

Businesses are already familiar with a raft of obligations under existing law throughout the data lifecycle. The GDPR toughens those obligations, and corresponding practices and policies will need review and updating. For example:

- new requirements for privacy notices, and information to be provided before personal data is collected, means existing consents need careful review for GDPR-compliance
- far more detailed obligations must be included in contracts with processors, meaning all existing processor agreements will need to be amended
- systems for responding to the rights of data subjects need to be more powerful

New obligations on data controllers

As well as global reach, the GDPR introduces new obligations that mean businesses may need to appoint a Data Protection Officer (DPO) and will need to train people, review processes and adapt technology, including to be able to:

- respond to data subject requests for data restriction, portability and the now-codified 'right to be forgotten'
- notify regulators within 72 hours, and data subjects without undue delay, of certain personal data breaches
- handle all dealings with children appropriately
- take ongoing measures and maintain records to prove compliance to regulators

Processors directly covered

For the first time, data processors have direct obligations and liability:

- direct obligation to implement appropriate security measures
- designating a DPO and / or representatives within the EU when required
- restrictions on the use of sub-processors
- liability for infringement of the GDPR's processor provisions
- liability for acting contrary to the controller's instructions

How can we help?

Whether you're looking for assistance with general or specific concepts, tackling your GDPR compliance project, reviewing your processing arrangements, training your staff or modelling your ongoing governance and compliance processes, contact us to see how AmberGate™ can help.

With over 20 years of experience advising on the commercial interpretation of data protection laws and guidelines, AmberGate is highly skilled in interpreting the regulatory environment into actionable and manageable risk-managed-based compliance programs in this core risk (and reward) arena.

Contact us now:

AmberGate Know-How Limited
86-90 Paul Street
London EC2A 4NE

T: +44 (0)20 3870 2636
E: info@ambergate.io

[1] https://ico.org.uk/media/action-weve-taken/mpns/1625131/mpn-talk-talk-group-plc.pdf
[2] https://ico.org.uk/media/action-weve-taken/mpns/2014626/mpn-talktalk-20170807.pdf