Performance Plus™ Partnership
Enabling Business Excellence

GDPR

Everything[1] You Always Wanted to Know[2] about GDPR[3] But Were Afraid to Ask[4]

1. Well at least some things – after all, who knows everything?
2. You may not have actually wanted to know these things but it's more of a case of you really needing to know them
3. This would include what the initials GDPR actually stand for and why you need to know these things now and not in a few years time
4. We're not for one moment suggesting that you're a scaredy-cat but, let's face it, sometimes you just don't want people to know that you don't know these things. Of course, in reality they probably don't know either, so by reading this little booklet you can potentially revel in the fact that you know something that they don't (whoever they are) – or you could of course pass this booklet to them so that they know as well

Caveat (The Small Print)
Information given in this little booklet is intended as a (very) brief guide to the GDPR and why UK businesses should be aware of the regulation and some of the things they should be doing right now to ensure compliance with it – because the penalties for not doing so are downright horrendous.

It is not by any means a complete explanation of the regulation, nor is it in any way a substitute for professional or legal advice on the subject, so if in doubt go out and find some of that advice and pay for it, it's considerably cheaper in the long run.

Contents

PerformancePlus Document Ref GDPR02/2017 Issue #1
Author David Baker

Introduction

The European Union (EU) General Data Protection Regulation (GDPR – now you know what the initials stand for) is an attempt by the EU to enforce a common standard for data protection across the whole EU and it applies to any organisation which has 'an establishment' within the EU where personal data is processed in the context of the activities of that establishment or, if the organisation does not have an establishment within the EU but nevertheless processes data about EU subjects in connection with the provision of goods or services or which monitors the behaviour of those data subjects. (A bit of a mouthful, but essentially **if you do business in the EU which involves holding or processing personal data then this regulation applies to you**)

Personal data in this context is any information relating to an identified or identifiable natural person (androids and zombies are currently excluded) and the definitions of identified or identifiable are pretty wide (including such things as 'online identifiers' or location data). The GDPR also identifies some specific types of personal data which require special care and consideration – these include data relating to race, sex, religion, genetic or biometric data, health, political opinion, criminal convictions and trade union membership (amongst others).

The fact that the GDPR is a regulation means that it has a direct effect on member countries without the need for any changes in the law of those countries and when it comes into force it will immediately supersede any local laws pertaining to Data Protection that had previously been in force.

The GDPR comes into force on the 25th May 2018 and irrespective of the fact that the UK has voted to leave the EU it will also apply to the UK because on that specific date the UK will still be a full member of the EU. Putting this another way – the GDPR will come into force in the UK on the 25th May 2018 and **if your organisation is already subject to the UK Data Protection Act of 1998 then the GDPR definitely applies to you and you had better be ready for it**.

The Underlying Principles of the GDPR

The GDPR sets out 6 data protection principles which largely mirror those of the existing UK Data Protection Act of 1998, these are:

- Personal data shall be processed **lawfully**, **fairly** and in a **transparent** manner in relation to the data subject
- Personal data shall be collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes (in other words you can't collect personal data for one reason and then later use it for something completely different)
- Any data collected shall be **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed
- Any data collected should be **accurate** and, where necessary, kept **up to date** and all reasonable steps should be taken to ensure that any inaccurate or out of date information is rectified or erased without delay
- Personal data should be **kept for no longer than is necessary**
- Data should be processed in a manner that ensures its **security, integrity and confidentiality**

In addition the GDPR states that the **Data Controller shall be responsible for and be able to demonstrate compliance with the regulation**

Consent

The GDPR is quite specific insofar as the consent given by the data subject with regard to the collection and use of their personal data. It states that this consent must be:

- Freely given, specific, informed and unambiguous
- Kept separate and distinct from other terms and conditions
- As easy to withdraw as to be given (and can be withdrawn at any time)

Specifically, Data Controllers cannot rely on consent by default or any form of 'bundled consent' that might have been relied on previously and consent cannot be made as a direct requirement for the supply of products or services. There are also some specific provisions in respect of children's consent and/or the processing of children's data

Transparency

Data Controllers are required to provide data subjects with information notices which contain certain prescribed information about how their personal data is processed, this includes:

- The identity and contact details of the Data Controller (and the Data Protection Officer if applicable)
- The purposes of the data processing
- The categories of personal data being processed
- The length of time the personal data will be kept
- Details of any other parties with whom the data is to be shared and any other countries (outside the EU) where the data will be transferred (and any safeguards on the use or transfer of the data)
- The data subject's right to withdraw consent at any time
- The data subject's right to lodge a complaint with a supervisory authority
- Whether there is any legal requirement to provide personal data

Accountability

The GDPR introduces a new principle that requires that Data Controllers are able to demonstrate compliance with the regulation which includes:

- Keeping detailed records of processing activities
- Performing data protection impact assessments for high risk processing
- Designating a named Data Protection Officer
- Notifying and recording data breaches
- Implementing data protection by design and default

Notably, the records must be in writing (printed or electronic forms) and must be made available to the supervisory authority on request. Having said this, the record keeping obligations don't technically apply to organisations employing fewer than 250 persons unless the data processing is:

- Likely to result in a risk to the rights and freedoms of the data subjects
- The processing is not occasional
- The processing includes special categories of data or data relating to criminal convictions or offences

Data Protection by Design

This is a new requirement (in comparison to existing UK Data Protection requirements) insofar as it requires organisations to build data protection into their data processing activities right from the initial design phase. It requires that organisations take protection measures that are appropriate by reference to the state of the art, the cost of implementation and the nature, scope, context and purposes of the data processing.
It further states that **organisations may use an approved certification scheme (for example ISO27001) as an element to demonstrate compliance with the requirement to apply data protection by design**

Data Subject Rights

The GDPR builds on existing Data Protection laws by enhancing data subject rights and adding a number of new rights.

Current rights include:

- The right to rectification of personal data
- The right to restrict processing of personal data
- The right of subject access to personal data
- The right not to be subject to automated decision taking including profiling

New rights brought in by the GDPR include:

- The right to transparency
- The right to data portability
- The right to erasure of personal data (sometimes known as the right to be forgotten)

A significant change to the right of subject access to personal data is that organisations are no longer entitled to charge a £10 fee to respond to subject access requests and must now respond to such requests within 1 month

Breach Notification

The GDPR brings far more stringent requirements to breach reporting, namely:

- Breaches must be reported by Data Controllers to supervisory authorities within 72 hours of the Controller becoming aware of the breach
- Breaches must be reported by Data Controllers to data subjects without undue delay unless a specific exemption applies e.g.

- If the personal data affected by the breach is unintelligible (i.e. it is encrypted)
- If measures have been taken to ensure that no high risk to the rights and freedoms of the data subject will materialise
- It would involve disproportionate effort to provide individual notification (in which case a public communication of the facts could suffice)

Enforcement and Sanctions (the downright horrendous stuff!)

Supervisory authorities (such as the ICO) will retain broad investigative and enforcement powers under GDPR which will enable them to conduct on-site audits, issue public reprimands and warnings and remediation orders

Under the GDPR there is a significant increase to potential fines of up to €20 million or 4% of total worldwide annual turnover (whichever is the greater) for major breaches

Of perhaps even greater significance (if there can be something of greater significance to an organisation than a €20 million fine!) is the fact that the GDPR makes it far easier for individuals to bring private claims against both Data Controllers and Data Processors and, further, allows the right for the data subject to claim compensation for distress and hurt feelings where no financial loss has been suffered. **The likelihood of this particular feature spawning a whole new industry of no-win, no-fee litigation claims against data processing organisations is, we fear, a virtual certainty.**

PerformancePlus and how we can help you

At PerformancePlus we believe that what our clients want to do is to run their own businesses in the most efficient and effective way that they can and not be burdened by excessive bureaucracy and paperwork. On the other hand those same clients typically also require some form of international certification showing that their systems (whether they are in respect of quality, environment, health & safety or information security) are the best that they can make them and conform to those accepted international standards.

We help our clients to create and maintain practical framework systems that are both comprehensive in relation to the chosen international standards and yet are easy to operate and that not only help them to achieve certification but also enable them to run their businesses more efficiently and more effectively.

GDPR is a regulation that will be enshrined in UK law in 2018 and it is incumbent on all organisations that store and/or process any form of personal data to comply with that law – and if they haven't started thinking about it yet then time is definitely running out.

PerformancePlus can help your organisation to comply with the GDPR by helping you towards certification under the ISO27001 Data and Information Security standard. At the very least, we can perform an initial data security audit on your organisation which will highlight any major discrepancies and allow you to start making changes well before the GDPR becomes law.

And best of all, our charges are far, far lower than a €20 million fine!

Contact us on 01284 330 400 or sales @performanceplus.co.uk