PKE CONSULTANTS

PUBLICATION SHEET No. 1 15 May 2018

General Data Protection Regulation (GDPR)

Introduction

After four years of preparation and debate the GDPR was finally approved by the EU Parliament on 14 April 2016. Enforcement date: 25 May 2018 - at which time those organizations in non-compliance may face heavy fines.

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. The key articles of the GDPR, as well as information on its business impact, can be found throughout this site.

The GDPR rules apply to almost all private sector processing by organisations in the EU or by organisations outside the EU which target EU residents. The export regime will ensure their impact is felt where such organisations transfer personal data to the EU. The maximum fines for non-compliance are the higher of €20m and 4 per cent of the organisation's worldwide turnover.

The concept of accountability is at the heart of the GDPR rules: it means that organisations need to be able to demonstrate that they have analysed the GDPR's requirements in relation to their processing of personal data and that they have implemented a system or programme that allows them to achieve compliance.

GDPR will also involve maintaining compliance for any data stored in the US Privacy Shield (the successor to Safe Harbour) when storing data in the US. Privacy Shield has already been implemented, but will be reviewed by the Article 29 Working Party (WP29) in summer 2017, and there will be more guidance as to its implementation.

What constitutes personal data?

Any information related to a natural person or "Data Subject" that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

What are the penalties for non-compliance?

Organizations can be fined up to 4% of annual global turnover for breaching GDPR or €20 Million. This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

What is the difference between a data processor and a data controller?

A controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes, conditions and means of the processing of personal data, while a processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Do data processors need 'explicit' or 'unambiguous' data subject consent - and what is the difference?

The conditions for consent have been strengthened, as companies will no longer be able to utilise long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent - meaning it must be unambiguous. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Explicit consent is required only for processing sensitive personal data - in this context, nothing short of “opt in” will suffice. However, for non-sensitive data, “unambiguous” consent will suffice.

What is the difference between a regulation and a directive?

A regulation is a binding legislative act. It must be applied in its entirety across the EU, while a directive is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to decide how. It is important to note that the GDPR is a regulation, in contrast to the previous legislation, which is a directive.

Does my business need to appoint a Data Protection Officer (DPO)?

DPOs must be appointed in the case of:

a) public authorities (except for courts acting in their judicial capacity),
b) organizations that engage in large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking), or
c) organizations that engage in large scale processing of special categories of data, data relating to criminal convictions and offences, and sensitive personal data (Article 37 of GDPR). If your organization doesn't fall into one of these categories, then you do not need to appoint a DPO.

For further information on when you need to appoint a DPO, please refer to the ICO Guidance.

What if your organisation falls outside the scope of having a DPO?

If your organisation falls outside of the scope to have a mandatory DPO, there is still a requirement under the new regulation for you to ensure that your organisation has sufficient staff and resources to discharge your obligations under the GDPR. This can be achieved by appointing a Data Compliance Officer (DCO). A DCO is best defined as an individual designated with the role of ensuring compliance with any regulatory requirements and is known to be the point of contact across the organisation who will be expected to handle any events that materialise in respect of data protection.

How does the GDPR affect policy surrounding data breaches?

Proposed regulations surrounding data breaches primarily relate to the notification policies of companies that have been breached. Data breaches which may pose a risk to individuals must be notified to the DPA within 72 hours and to affected individuals without undue delay.

What should I review to be compliant to GDPR?

Here are just a few of the areas of data management, and risks, need to review as part of your work based on GPDR Guidelines:

ORGANISING STAFF

- Identify who in your organisation needs to be aware that data law is changing
- Designate a data protection officer if required (see GDPR for guidelines), for examining data protection compliance
- If your business has interests in the US, ensure all relevant staff are aware of the US Privacy Shield

INTERNAL SYSTEMS

- Consider whether your business needs a risk register, or revisit the existing one
- Review current privacy notices in accordance with the ICO guidelines on GDPR
- Check that procedures cover all the new rights that individuals have under GDPR
- Work out whether you need to organise an information audit and if so across how much of the business
- If appropriate, ensure you have GDPR-specific procedures in place for gathering young persons' data
- Ensure you can detect a data breach and report and investigate it in a timely fashion, and ensure you have a policy in place to react on this breach, in accordance to new data breach reporting deadlines set under GDPR. Also, you should ensure that everyone aware of the data breach policy throughout the organisation.
- Look at ICO guidance on Data Privacy Impact Assessments (DPIAs) – assess situations where you will be required to conduct a DPIA and what procedures you will put in place
- Run relevant security checks to ensure your systems are robust around storage of said data in the run-up to May 2018
- Make sure that your IT team is effectively monitoring your security environment, and reporting to management on risks and improvements. The most effective way to do this is to carry out a regular checklist assessment of your systems, covering a wide range of topics such as;
- Network architecture and on-going changes
- Software updates – security/anti-virus and day to day operational applications

DATA PROCESSES

- Document what personal data you hold, where it came from, where within your organisation this information is maintained and managed and who you share it with
- Ensure that you have a process in place to delete client data if requested to do so by the client
- Review the process that will allow a client to take a copy of the data specific to themselves if requested to do so
- Look at the data processing you carry out – identify the legal basis for carrying tasks out and document them
- Review how you are seeking, obtaining and recording consent in line with GDPR – you must be able to demonstrate consent was given for processing the clients' data and this cannot be inferred from silence or gained from pre-ticked boxes (Questions to have in mind: Have the clients and affiliates approved to receive communications? Have you made it easy for people to manage mailing preferences? Are you recording the opt-ins obtained so you have a record of these?)

- Work out who all the data controllers and data processors in your business are, whether you use third parties to process information on your behalf, and plan any relevant training programmes for staff accordingly
- Does staff work on client data on a network or locally? If locally, what are the rules about retaining data files such as Word documents, spreadsheets and PDF files?
- Is your network secure from malicious attempts to access it? Have you considered strengthening the way that your staff identify themselves on your network?
- How are your firms laptops secured when staff are travelling?
- Are data storage devices (e.g. USB data sticks) managed and secured properly?
- Are your systems encrypted?
- What happens to emails coming into the office that contain attachments? Remember that forwarding an email replicates the data, and inevitably increases risks.
- Do you have a 'clear desk' policy?
- Does your software achieve the goal of 'Protection by Design'?
- Ensure the process to obtain consent to personal data from customers/clients is clear, understandable and consistent. Make sure you have clear policies around data retention and that they are understood and applied by all across the organisation.
- Do your existing procedures and policies cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format?
- Enforcement of building security and visitor access rules
- Management of leavers and joiners and the application of appropriate policies

STAKEHOLDERS

- Contact clients to inform/remind them of GDPR obligations and how your data privacy procedures and processes may be changing
- Keep a log of all clients who have been contacted
- Speak to your stakeholders, suppliers and third-party processors about the data you share and their timetables for GDPR implementation.
- Assess the risks around timeframes that conflict with your own preparations

Disclaimer