Simplifying Compliance

Introduction to GDPR eBook

Table of Contents

Introduction

This eBook has been created to provide an overview of the key themes of the General Data Protection Regulation (GDPR) to help organisations understand the new legal framework in the EU.

Purpose is to explain the similarities with the existing UK Data Protection Act 1998 (DPA), and describe some of the new and different requirements.

This document includes helpful links to relevant sections of the GDPR itself, to ICO guidance and to guidance produced by the EU's Article 29 Working Party.

General Data Protection Regulation (GDPR) applied in the UK since **25 May 2018**.

Organisations that have day-to-day responsibility for data protection must be 100% compliant, or face substantial fines for non-compliance.

Understanding GDPR

What is the GDPR?
The General Data Protection Regulation (GDPR) a new data protection regulation that became law across the EU since May 2018. It replaced all previous data protection regulations including Data Protection Act 1988, which was amended by the Data Protection (Amendment) Act 2003.

The GDPR regulations give consumers greater control over how their personal data is captured and used by with the vision of advanced trust in the digital economy.

Why the need for GDPR?
There has been major advancement in technology, and with the enormous growth in the volume of consumer data used and stored by businesses across the EU since the DPA amendment in 2003.
With the increase use of social media, Google, Facebook, Twitter and LinkedIn etc. current regulations were deemed no longer fit for purpose for the digital world.

Where does the GDPR apply?
The new regulation covers all businesses operating in the EU.
No single state will be subject to less or more regulation than any other state, making legislation more equal.
The new regulation also applies to any personal data of EU citizens which is stored outside the EU.

Who does the GDPR apply to?
The Controller is responsible for how and why personal data is processed.
The Processor who acts on behalf of the Controller is required to maintain records of personal data and processing activities. As a new requirement under the GDPR, the Processor will have significantly more legal liability for a breach.
The GDPR places further obligations on the Controller to ensure contracts with Processors comply with the GDPR.

Penalties for non-compliance

What are the penalties for non-compliance?
Organisations 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.

Three of the biggest data breaches of 2020 (so far)

January - Marriott International
Estimated 5.2 million of guest information was obtained by hackers using the login credentials of two Marriott employees.
Cyber hackers likely used credential stuffing (compromised passwords) using may have taken guests personal details such as names, birthdates, telephone numbers, and loyalty account numbers.
It's unsure if details included passwords or PINs for payment card details, passport information, national IDs or driver's license numbers.

Information Commissioner's Office (ICO) proposed a GDPR penalty fine of $124million for the breach that wasn't discovered until late February

April – Nintendo
The Japanese video game company acknowledged that around 160,000 accounts were exposed after the Nintendo Network ID (NNID) system was compromised
Users reported unauthorised logins to their accounts, and fraudulent use of stored credit card data.
The security incident led to the leak of personal identifiable information such as nicknames, date of birth, country, region, email address and gender.

It has not been announced what if any GDPR fines ICO will propose.

May – EasyJet
EasyJet first became aware of the phishing attacks in January, but admitted in May that a "highly sophisticated cyber-attack" affecting nearly 9 million customers.
Email addresses, travel details and credit and debit card details had been "accessed".

It told the BBC that it was only able to notify 2,208 customers whose credit card details were stolen in early April. Stolen credit card data included the three digital security code, known as the CVV number on the back of the card.

ICO are continuing to investigate this breach, and EasyJet may face investigation by other relevant authorities. It is also facing a potential group litigation claim of up to £18 billion in respect of the breach.

Key Areas

Lawful processing
Under the GDPR, you need to identify and document a legal basis before you can process personal data. This is referred to as the “conditions for processing” under the DPA.

Consent
The GDPR references to both ‘consent’ and ‘explicit consent’.
Both forms of consent have to be freely given, specific, informed and an unambiguous indication of the individual’s wishes.
Consent under the GDPR requires some form of clear affirmative action. Silence, pre-ticked boxes or inactivity does not constitute consent.
A record must be kept of how and when consent was given, and Individuals have a right to withdraw consent at any time.

Rights for individuals
There are new rights for individuals and current rights under the existing DPA have been strengthened.

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Accountability and governance
The GDPR includes provisions that promote accountability and governance.
These complement the GDPR's transparency requirements.
Organisations are expected to put into place comprehensive but proportionate governance measures.
Good practice tools such as privacy impact assessments and privacy by design are now legally required in certain circumstances.
These measures should minimise the risk of breaches and uphold the protection of personal data.

Breach notification
The GDPR will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected.

- **Personal data breach**
  A breach is more than just losing personal data.
  A breach of security that leads to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

- **Notify the relevant supervisory authority**
  You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals.
  If unaddressed, such a breach is likely to have a significant detrimental effect on individuals that results in discrimination; damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage e.g. a loss of customer details where the breach leaves individuals open to identity theft.

- **Notify individuals**
  Where a breach is likely to result in a high risk (the threshold for notifying individuals is higher than notifying the relevant supervisory authority) to the rights and freedoms of individuals.
  You must notify those individuals concerned directly.

- **How to notify a breach**
  A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it.
  The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.
  If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.
  Failure to notify a breach when required to do so, can result in a significant fine up to 10 million Euros or 2 per cent of your global turnover.

- **How to prepare for breach reporting**
  Businesses should make sure that everyone in their organisation understands what constitutes a data breach, and a data breach is more than a loss of personal data.
  You should ensure that you have an internal breach reporting procedure is in place. This will facilitate decision-making about whether you need to notify the relevant supervisory authority or the public.
  In light of the tight timescales for reporting a breach - it is important to have robust breach detection, investigation and internal reporting procedures in place.

Transfers of personal data
To ensure that the level of protection of individuals is not undermined, the GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

Infrequent or one-off transfers of personal data concerning relatively few individuals the GDPR provides that personal data may still be transferred outside the EU where the transfer:

- Is not being made by a public authority in the exercise of its public powers.
- Is not repetitive (similar transfers are not made on a regular basis).
- Involves data related to only a limited number of individuals.
- Is necessary for the purposes of the compelling legitimate interests of the organisation and provided such interests are not overridden by the interests of the individual.
- Is made subject to suitable safeguards put in place by the organisation to protect the personal data.

In the above cases organisations are obliged to inform the relevant supervisory authority of the transfer and provide additional information to individuals.

National derogations
Member States can introduce exemptions from the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- National security.
- Defence

- Public security
- Prevention, investigation, detection or prosecution of criminal offences
- Other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security.
- Protection of judicial independence and proceedings
- Breaches of ethics in regulated professions
- Monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention
- Protection of the individual, or the rights and freedoms of others or the enforcement of civil law matters

Member States can provide exemptions, derogations, conditions or rules in relation to specific processing activities, include processing that relates to:

- Freedom of expression and freedom of information.
- Public access to official documents.
- National identification numbers.
- Processing of employee data.
- Processing for archiving purposes and for scientific or historical research and statistical purposes.
- Secrecy obligations.
- Churches and religious associations.

Data Governance

While the GDPR regulation is clear on what needs to be done, many organisations are struggling with how to do it.

Data governance can serve as the underpinning of GDPR compliance. It provides a framework for managing and defining enterprise-wide policies, business rules, and data assets to deliver the necessary level of data protection and quality.

The Data Governance Institute (DGI) provides in-depth, vendor-neutral Data Governance best practices and guidance. Since its introduction in 2004, the DGI Data Governance Framework has been employed by hundreds of organizations around the globe.

To comply with GDPR many organisations will need a new approach and new tools for data protection and privacy.

Manual approaches and spreadsheets will not suffice; neither will another ‘bolt-on’ IT system.

Navigating the requirements of GDPR is no small feat, but you don’t have to go it alone……

Next steps

P4P Compliance Management Limited can help organisations prove that they are always doing the right thing with the data.
Contact us for GDPR, Data Governance and Data Security advise.
Email: enquire@p4p.uk.com

Useful links

ICO
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-be-informed/

Data Governance
http://www.datagovernance.com/