General Data Protection Regulation (GDPR) Briefing

This document is provided for our Registrants and Member Institutions as general guidance and information on the main principles in relation to GDPR; it does not cover all elements of the new legislation. The new GDPR legislation is a complicated area of law and we advise that you visit the ICO[1] website for further in-depth guidance. You may also wish to speak to a qualified GDPR practitioner or your professional insurers to ensure that you are legally compliant under the new legislation.

Table of Contents

[1] The Information Commissioners Office – the statutory body that oversees data protection issues

Introduction

"GDPR is an evolution in data protection, not a burdensome revolution". [2]

"The GDPR is at root a modernisation of the law"[3]

The General Data Protection Regulation (GDPR) becomes effective from **25 May 2018** and will apply to all European states. Many of the fundamental principles of the GDPR remain the same as the Data Protection Act 1998, however the GDPR replaces the Data Protection Act and enhances many rights and obligations.

Despite Brexit, the Government has confirmed its intention to bring the EU GDPR into UK law, to ensure the country's data protection framework is suitable for the modern digital world and allows data subjects better control of their data.

Aim of GDPR

The aim of GDPR is to protect all EU citizens from privacy and data breaches in an increasingly digital, social media and technological world. The digital world now is vastly different from the time in which the data protection law was first established. The new legislation works in setting a standard across all member states in relation to data laws and compliance. In summary the GDPR changes the way in which data controllers handle personal information and gives individual's enhanced rights of protection when it comes to their personal data.

Will GDPR apply to me?

As a BPC registrant or a BPC Member Institute and you hold personal data then the GDPR law will most likely apply to you. Personal data includes names and addresses of individuals. Most organisations and service providers will come under the GDPR legislation. If as a BPC registrant you're a sole trader working from home and carrying out a commercial activity and collect personal data, the GDPR legislation will most likely apply to you.

[2] ICO website
[3] ICO website

Do I need to register with the Information Commissioners Office (ICO)?

If you handle personal data, under the old data protection rules you had to register as a data controller with the ICO. Under the GDPR there is no longer an obligation to register with ICO for data processing. However an individual/organisation will now need to pay the ICO a data protection fee.

The fee structure is still being developed and more information can be found here

Key definitions to understand GDPR Law

Personal data includes any information relating to an identified or identifiable natural person;

This definition provides for a wide range of personal identifiers to constitute personal data;

a) Name;

b) Identification number;

c) Location data or online identifier.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Sensitive Personal data contains information about the following;

a) Racial or ethnic origin;

b) Sex life or sexual orientation;

c) Political opinions;

d) Health - Physical or mental health condition;

e) Religious beliefs;

f) Trade union membership;

g) Criminality, alleged or proven.

Processing personal data '**processing**' Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use,

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Subject A natural person who can be identified directly or indirectly, in particular by reference to an identifier under the heading personal data as set out above.

Data Controller A controller determines the purposes and means of processing personal data.

Data Processor A processor is responsible for processing personal data on behalf of a controller. This will apply if an individual contracts out to an agency to process personal data.

What changes does the GDPR Law bring in?

- **Accountability:** The GDPR promotes accountability and governance and the Independent Commissioners Office (ICO) states that arguably the new law brings the biggest changes under the heading of accountability. The GDPR requires organisations/individuals to not only adhere to GDPR legislation but also show compliance of the legislation. The legislation obligates organisations/individuals to:

    a) Maintain an internal record of all processing activity;
    b) Record the purpose of the processing;
    c) Keep a description of the technological or organisational measures to ensure a level of security.

- **Lawful processing of personal data –** The GDPR requires individuals/organisations to identify the lawful basis for processing the personal data. The categories of lawful bases under the GDPR are broadly the same as the conditions for processing under the Data Protection Act. Organisations/individuals should review the types of processing activities that they carry out and identify the lawful basis for doing so. The categories as set out under Article 6 of the GDPR include the following;

    (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

    (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

    (c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

    (d) Vital interests: the processing is necessary to protect someone's life.

    (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

    (f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the

individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)[4]

A data controller will need to identify, record and set out the lawful basis in their privacy notice. A privacy notice is a statement that discloses some or all of the ways a data controller, uses, discloses, and manages a customer or client's data. Being transparent and providing accessible information to individuals about how you will use their personal data is a key element of the GDPR. The most common way to provide this information is in a privacy notice.

- **The Rights of individuals** - Data subjects: The rights of individuals have been enhanced under the GDPR in many areas.

    a. Individuals have the right to be informed about the collection and the use of their data.
    b. Individuals should be notified of the following: Purpose of the data collection, retention periods, the lawful basis for the procession and with who the data will be shared. (This can be done in a privacy notice as set out above.)
    c. Note: You must provide individuals with the privacy notice/information when you first collect the data.
    d. The information you provide to individuals must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

- **Right of access**: Individuals will have the right to obtain from organisations/individuals their personal data along with supplementary information. They also have the right to know whether an organisation is processing their personal data.

    a. Subject access requests - Will have to be responded to within 40 calendar days of the request. The copies of the personal data will need to be provided free of charge unless the request is manifestly unfounded or excessive.

    b. The right to rectification - An individual has a right to rectification of their details if their details are incorrect. The time limit for correcting the information is one month and should be free of charge. The time length can be extended to two months if the request is complex.

    c. An individual has a right to be forgotten:

        1) Where the personal data is no longer necessary to achieve the purpose it was collected or otherwise processed.
        2) The individual withdraws consent on which the processing was based upon and where there is no other lawful basis for processing.
        3) The individual objects to the processing and there are no overriding legitimate grounds for the processing.
        4) The personal data has been unlawfully processed.
        5) The personal data has to be erased for compliance with a legal obligation.

[4] ICO website

d. Data portability – The right for data subjects to ask for their personal data to be handed back or sent to another data controller. You must provide the personal data in a structured, commonly used and machine readable form.

- **Personal data breaches** – A personal data breach includes the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

    a. The GDPR imposes a duty to report certain types of personal data breaches to the ICO unless the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals. This must be done within 72 hours of becoming aware of the breach.
    b. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you should also inform those individuals without undue delay.
    c. Individuals/organisations should ensure that they have breach detection, investigation and internal reporting procedures in place. This will facilitate decision making about whether or not you need to notify the ICO and the affected individuals.
    d. Individuals/organisations should record any personal data breaches, regardless of whether they are required to notify the ICO.

- **Penalties for non compliance** - The GDPR introduces mandatory reporting of breaches to the ICO and affected individuals, where individuals are put at risk. The penalties have been increased:

    a) €20m or 4% of turnover for a breach of data protection principles or data subjects' rights.
    b) €10m or 2% of turnover for administrative failures, such as failure to report a breach.

  The fines are discretionary and will apply on a case by case approach.

- **Consent** – The GDPR sets a higher standard for consent. Consent means offering individuals real choice and control. Individuals/organisations should check their current consent practices and existing consent already obtained in order to ensure compliance. Consent must;

    a) Require a positive opt-in; don't use pre-ticked boxes or any other method of default consent.
    b) Be specific; relate to one or more specific purpose;
    c) Be informed;
    d) Be clear and concise;
    e) Avoid making consent to processing a precondition of a service;
    f) Keep your consent requests separate from other terms and conditions.
    g) Be easily withdrawn if the data subject has a change of mind. Information should be provided in relation to withdrawing consent.

Individuals/organisations are not required to automatically 'repaper' or refresh all existing Data Protection Act consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, you will need to make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR compliant consent, or find an alternative to consent.

- **Sensitive personal data** - The GDPR is further enhanced to include genetic data and some biometric data in the definition of sensitive personal data. Further this definition does not include personal data relating to criminal offences and convictions, as there are separate and specific safeguards for this type of data in Article 10 of the GDPR. In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These do not have to be linked. Further information can be found on the ICO website on the particular Articles.

- **Children's personal data -** The GDPR legislation enhances the protection of a child's personal data. All privacy notices should be written in plain language so that the child can understand it.

How can I prepare for GDPR?

- Determine what personal data that you hold, carry out a data audit.
- Ask yourself what is your legal basis for processing personal data? Identify this and record it.
- Ensure that you have met the criteria in order to process sensitive personal data.
- Think how you communicate privacy and update privacy notices according to the new requirements of GDPR.
- Improve your internal processes in terms of storage /electronic data to ensure that you are GDPR compliant.
- Check the language you use when gaining consent and whether you will need to refresh consent.
- Be ready to respond to subject access requests and have clear electronic and paper filing systems in order to meet the deadline when a request is submitted.
- Ensure you have a clear system in place in order to pick up data breaches and record and report them if required.
- Check what personal data that you hold and whether you are still permitted to hold it. Retention of documents is very important under the GDPR, review the length of time you keep personal data;
- Consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
- Securely delete information that is no longer needed for this purpose or these purposes; and update, archive or securely delete information if it goes out of date.

Further Information

The above information is a brief insight on the key areas of GDPR it is not substantive review and we advise that you visit the ICO website for further information. Please find the link for the ICO website:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The ICO have a 12 step guidance document which is useful when preparing for the new legislation.

Please find link below:

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

The ICO also has dedicated help lines that can be found at: https://ico.org.uk/global/contact-us/