THE GENERAL DATA PROTECTION REGULATION

BEAUCHAMPS

BEAUCHAMPS

Last updated: Beauchamps December 2017

THE GENERAL DATA PROTECTION REGULATION

Contents

INTRODUCTION

On 25 May 2018, the General Data Protection Regulation (the **GDPR**) will become law across all member states within the European Union.

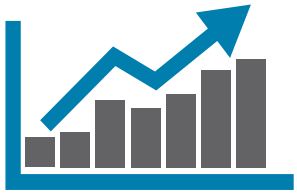
It has been widely described as a "game-changer" as it overhauls the manner in which all businesses and organisations handle personal data. Significant penalties can be imposed for breaches so doing nothing is not an option.

GRPR is a reality for all businesses / organisations that hold data about individuals. It is not too late to start your GDPR preparations, including setting objectives, creating a project team and allocating a budget and resources. **The time to act is now.**

In this guide, we set out the key provisions of the GDPR and the key steps for organisations to take to ensure compliance with the GDPR by the deadline, as well as a "jargon buster" on the key terms relating to the GDPR.

THE GDPR AT A GLANCE:

Harmonised rules



Increased transparency, security and accountablity

Enhanced rights for individuals

Data Protection Officer

Privacy by design & default

Data protection impact assessments

Mandatory data breach notification

Increased penalties / right to compensation

What is the GDPR?

Its full title is "*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*", otherwise commonly known as the "General Data Protection Regulation" or the "GDPR".

Why is the GDPR so important?

The GDPR will overhaul the data protection legal framework in Europe when IT comes into effect on 25 May 2018 and Irish businesses must be fully compliant by that date.

The GDPR will apply a single set of rules that are valid across all EU Member States. As it is a Regulation, this means that it will be immediately enforceable in Ireland (and other Member States) without the need for domestic legislation. This should decrease the level of national variation but there will not be complete European wide uniformity as the GDPR has left discretion to Member States in a number of areas.

The GDPR emphasises transparency, security and accountability on the part of businesses (irrespective of their size) that collect and process personal data, while standardising and strengthening the rights of EU citizens. It will greatly increase obligations on businesses as well as giving data protection authorities more robust powers to tackle non-compliance including the imposition of significant financial penalties.

Compliance with the GDPR will place a greater administration and compliance burden on businesses. However, preparation is the key to a smooth transition to the new data protection standards. The sooner preparations commence, the easier it will be for businesses to transition to the new standards.

Re-cap of data protection rules

Data protection protects the privacy rights of individuals by placing responsibilities on businesses that process personal data. Businesses must adhere to the key data protection principles summarised below and must show that the processing of the data is necessary for a particular purpose(s), known as a "lawful basis", eg to perform a contract with the data subject or to comply with a legal obligation to which the business is subject. Businesses processing data must:

- Obtain and process personal data fairly
- Keep personal data only for one or more specified and lawful purposes
- Process personal data only in ways compatible with the purposes for which it was given to the business initially
- Keep personal data safe and secure
- Keep personal data accurate and up-to-date
- Ensure that personal data is adequate, relevant and not excessive
- Retain personal data no longer than is necessary for the specified purpose or purposes
- Give a copy of his / her personal data to any individual, on request

The GDPR builds on the above principles. However, it goes further for example by increasing standards and sanctions as well as introducing the principles of accountability (eg business must be able to demonstrate compliance with the GDPR) and transparency (eg any information / communication provided by businesses relating to the processing of personal data must be easily accessible, easy to understand and be in clear and plain language). The GDPR also amends and restates the permitted lawful bases for processing data.

The Data Protection Commissioner enforces data protection law in Ireland. The Government has however indicated its intention to replace the Commissioner with a "Data Protection Commission" which will be the "supervisory authority" under the GDPR (commonly known as the "data protection authority" (**DPA**)) who will monitor the application of and enforcement of the GDPR.

A jardon buster of terms is included at the back to explain, in layman's terms, some of the language used.

What are the key provisions of the GDPR?

- It has extra-territorial effect which means that it will apply to controllers and processors based outside the EU
- Requirement to appoint a Data Protection Officer in certain circumstances
- Stricter requirements for valid consent to data processing
- Enhanced rights for individuals
- Reduced time period for dealing with individual's rights
- Obliging businesses to be clearer about how they use personal data
- Mandatory Data Protection Impact Assessments in certain circumstances
- Notification of data breaches within 72 hours of occurrence
- Data protection by design and default
- Right to Compensation for individuals
- New obligations for processors
- Increased penalties for non-compliance
- Ability to appoint a Lead Supervisory Authority (**LSA**)

1.EXTRA-TERRITORIAL EFFECT

The GDPR has extra-territorial effect. Firstly, it applies to the processing of personal data by an EU business regardless of whether or not the processing takes place in the EU. This means that an EU business who uses servers outside the EU may fall within the scope of the GDPR.

Secondly, it applies to all non-EU businesses that process personal data of EU citizens relating to the offering of goods / services to such citizens (irrespective of whether payment is required) or monitor the behaviour of such citizens in the EU. Such businesses will be obliged to appoint an EU-based representative.

Where a controller or processor has more than one establishment (eg office) in the EU, the GDPR recognises the 'one-stop-shop' through the concept of a 'main establishment' with a single lead supervisory authority (see point 13 for further details).

2. DATA PROTECTION OFFICER (DPO)

Businesses will need to decide if they need to appoint a DPO. The following entities must appoint a DPO:

- public authorities
- businesses that engage in large scale regular and systematic monitoring of individuals, and
- businesses that engage in large scale processing of special categories of personal data (see jargon buster on page 17) or data relating to criminal convictions / offences

Even if the GDPR does not require the appointment of a DPO, some businesses may appoint a DPO on a voluntary basis. The GDPR rules relating to DPOs apply whether the appointment is voluntary or mandatory. Where a business is not required to appoint a DPO and tasks a person with responsibility for GDPR compliance, care should be taken to ensure that that person is not deemed to be a DPO, as this will give rise to the additional GDPR obligations.

As stated above, all public authorities must appoint a DPO and it is possible for a single DPO to be designated for several public authorities, taking account of their organisational structure and size. It is also possible for a single DPO to represent a number of private businesses.

In Guidelines adopted on 13 December 2016 and revised on 5 April 2017, the Article 29 Working Party (**Working Party**) recommends that unless it is clear that a controller or processor is not required to designate a DPO, then controllers and processors should document the internal analysis carried out to determine whether or not a DPO is to be appointed in order to be able to demonstrate that the relevant factors have been taken into account properly.

The role of a DPO is to advise the business (be it a controller or processor) on its obligations under, and to monitor compliance with, the GDPR. They will also cooperate with and act as a contact point for the DPA. They should report to the highest management of the business, be independent and can fulfil other tasks as long as there is no conflict of interests. They should have expert knowledge of data protection law and practices. The DPO may be a member of staff or it may be outsourced.

Whoever the person is, the DPO must receive sufficient resources (ranging from financial to infrastructure and staff) in order to carry out its tasks.

The DPO must be involved in all issues which relate to the protection of personal data within the business, in particular by organising training and establishing a network of persons who are aware of the data protection issues within the organisation. They are also bound by confidentiality.

DPOs are also the contact point for individuals within or outside the organisation with regard to all issues relating to the processing of their personal data and to the exercise of their rights under the GDPR.

Businesses must not interfere with the DPO and they cannot penalise or dismiss the DPO in relation to the performance of his / her tasks. It is an offence for a business not to appoint a DPO where they are obliged to do so and they may be subject to fines.

3. CONSENT

The requirements around consent have been strengthened by the GDPR. This means that where a business intends to rely on consent for the lawful processing of personal data, they must be able to demonstrate that valid consent has been received from each individual whose personal data is being processed. To be a valid lawful basis for processing data, consent must be freely given, specific, informed, unambiguous and be in plain language. Individuals also have the right to withdraw consent at any time and it must be as easy to withdraw as to give consent.

Consent will not be regarded as freely given if the individual has no genuine or free choice or is unable

to refuse or withdraw consent without detriment eg in an employee / employer relationship. If processing has multiple purposes, consent should be obtained for each of them. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations. For consent to be informed, the individual should be aware of the identity of the controller and the processor and the purpose of the processing. An unambiguous indication of an individual's consent may include ticking a box when visiting a website or a statement or conduct which clearly indicates the individual's acceptance of the proposed processing of their personal data eg responding to an email requesting consent. Silence, pre-ticked boxes or inactivity will not constitute consent. The onus will be on the business to demonstrate that consent has been received and so a record should be kept which evidences consent.

Under the GDPR, the age of consent in relation to digital services is 16 but the Irish Government recently announced that it will lower this to 13 years. This means that businesses will need to get consent from the parent or guardian before they allow children under the age of 13 to access their online services.

Where special categories of personal data are processed (such as data relating to health, political opinions or religious beliefs) an individual must give explicit consent unless the business proposes to rely on another basis as set out in the GDPR to process the individual's personal data eg processing is necessary to perform obligations under employment, social security or social protection law.

4. ENHANCED RIGHTS FOR INDIVIDUALS

Under the GDPR, individuals have a right of access to their personal data, a right to rectify inaccuracies in their personal data, a right to have personal data erased in certain cases, a right to restrict processing of their personal data, a right of portability (**Data Portability Right**), a right to object to data processing and a right not to be subject to automated processing including profiling (**Right to No Profiling**).

- **Data Portability Right** –this allows individuals to receive their personal data from a business or have it transferred to another, where technically feasible. It only applies to personal data given to the business by the individual. An individual may only exercise the Data Portability Right where processing is based on consent or under a contract and the processing is carried out by automated means. The data must be provided by the business in a structured, commonly used and machine-readable format.
- **Right to No Profiling** - Individuals also have the right not to be subject to a decision based solely on automated processing, including profiling which is defined as:

"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

While an individual has the right not to be subject to profiling, this does not apply where the processing is authorised by European or Member State law (for example, if the individual is being investigated for fraud or tax evasion purposes); the processing is necessary for entering into or performance of a contract between the individual and a controller; or where the explicit consent of the individual has been obtained.

5. REDUCED TIME PERIOD FOR DEALING WITH INDIVIDUAL'S RIGHTS

When an individual makes a request (eg for access to their personal data), businesses must provide the relevant information without undue delay and within one month of receipt of the request. This has been reduced from 40 days. The one month period can be extended to two months where requests are complex or numerous.

Information must be provided free of charge but a business may charge a reasonable fee for any further copies requested by an individual or where access requests are manifestly unfounded or excessive taking into account the administrative costs of providing the information.

If a business refuses to respond to a request, they must, without delay and at the latest within one month, explain

why and inform the individual of their right to complain to the DPA and their right to seek a judicial remedy.

6. OBLIGING BUSINESSES TO BE CLEARER ABOUT HOW THEY USE PERSONAL DATA

Businesses must be more transparent as to how they use personal data and so must now provide information to individuals about its processing of their personal data unless the individual already has this information. The information to be provided includes the identity and contact details of the controller and its DPO (if any), the purpose of the processing as well as the legal basis for the processing as set out in the GDPR (eg processing is based on consent, processing is necessary to perform a contract etc) who are the recipients of the personal data, details of any transfers outside the EU, how long the data is held, the right to request access as well as rectification or erasure of their personal data and the right to lodge a complaint with the DPA (to name but a few).

This information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Where the processing is addressed to a child, the information or communication should be in clear and plain language that a child can understand.

7. Data Protection Impact Assessment (DPIA)

Where processing is likely to result in a high risk to the rights of individuals, businesses must carry out an assessment of the impact of the processing operations on the protection of personal data and must seek the advice of its DPO (if any) when carrying out a DPIA.

Examples of high risk activities include:

- the processing of special categories of personal data or personal data relating to criminal convictions and offences is on a large scale;
- systematic monitoring of a publicly accessible area on a large scale (such as use of a camera system to monitor driving behaviour on roads);
- systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing (including profiling) and on which decisions are based that produce legal effects concerning the individual, or similarly significantly affecting the individual (eg a business creates a national credit rating or fraud database).

Businesses will be obliged to consult with the DPA in advance of processing where a DPIA indicates a high risk, in the absence of any measure taken by the business to mitigate that risk.

A DPIA must include a description of the processing operations and their purpose, an explanation of the necessity and proportionality of the processing operations, an assessment of the risks to the rights and freedoms of the individuals and the measures taken to mitigate the risk (including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR).

8. DATA BREACH NOTIFICATIONS

When a personal data breach occurs, the business must (no later than 72 hours after becoming aware of it), notify the breach to the DPA unless the breach is unlikely to result in a risk to the rights of individuals. If the notification is not made with 72 hours, a reason for the delay must be furnished. For example, a breach that would not require notification to the DPA would be the loss of a securely encrypted mobile device, used by the business and its staff. Provided the encryption key remains within the secure possession of the business and it is not the sole copy of the personal data, then the personal data would be inaccessible to an attacker. This means the breach is unlikely to result in a risk to the rights of the individuals in question. However, if it later becomes evident that the encryption key was compromised or that the encryption software or algorithm is vulnerable, then the risk to the rights of individuals will change and notification to the DPA may be required.

If the breach is likely to result in a high risk to the individual, they should also be notified of the breach without delay in clear and plain language but notification is not required in instances where, for example, it would involve a disproportionate effort in which case, a public communication would suffice. By way of example, if an online business suffered a cyber-attack where usernames, passwords and the purchase history of its customers are published online by the attacker, this the breach is likely to result in a high risk to individuals and so, the business would have to notify the breach to those affected as well as to the LSA if it involved cross-border processing.

Processors of personal data are required to notify the controller without undue delay after becoming aware of a data breach and controllers must document all breaches. Notifications should include (i) the nature of the breach including the categories and approximate number of individuals concerned as well as the categories and approximate number of records concerned; (ii) the name and contact details of the DPO or other person where more information can be obtained; (iii) the likely consequences of the breach; (iv) the measures taken (or proposed to be taken) by the business to address the breach including measures to mitigate its possible adverse effects.

9. DATA PROTECTION BY DESIGN AND DEFAULT

The GDPR introduces the new concept of privacy by design and by default. This is intended to strengthen the protection of privacy by requiring businesses to build consideration of privacy into their product and service design processes.

Privacy by design requires businesses at the time of the determination of the means for processing and at the time of data processing itself, to implement appropriate measures (such as pseudonymisation) which are designed to implement data protection principles and to integrate the necessary safeguards into data processing in order to meet the requirements of the GDPR and to protect the rights of individuals. In doing this, businesses must have regard to:

- the state of the art
- the cost of implementation
- the nature, scope, context and purposes of the processing and
- the risks of varying likelihood and severity for the rights of individuals posed by the processing.

Privacy by default requires businesses to ensure that by default, only personal data necessary for each specific purpose of the processing is processed. This applies to the amount of personal data collected, the extent of processing, the period of storage and accessibility. In particular, such measures must ensure that by default personal data is not made accessible (without the individual's intervention) to an indefinite number of natural persons.

10. RIGHT TO COMPENSATION FOR INDIVIDUALS

An individual who has suffered damage as a result of an infringement of the GDPR has the right to receive compensation from a business for the damage suffered. To avoid liability, a business will have to prove that it was not in any way responsible for the event giving rise to the damage. If a business (as controller) engages another company (as processor) and both are responsible for the damage caused, they will be jointly liable. A business will be entitled to recover from the other company that part of the compensation which corresponds to their responsibility for the damage.

Individuals also have the right to make a court application to appeal certain acts and decisions of the DPA and may apply to court for relief against businesses where their rights have been infringed as a consequence of non-compliance with the GDPR.

11. NEW OBLIGATIONS FOR PROCESSORS

The GDPR strikes an even balance between controllers and processors by making them jointly and severally liable according to their respective responsibility for the harm caused by a breach of data protection law. Under the GDPR, direct statutory obligations are imposed on processors – this means that processors are subject to direct enforcement by the DPA, as well as fines and compensation claims by individuals for any damage caused by breaching the GDPR. This is a significant change as currently processors only have to comply with the terms of the processing contract which they have agreed with the controller.

The GDPR also requires certain mandatory terms to be included in a contract between a controller and processor such as requiring a processor to only process data on the documented instructions of the controller, to sub-contract only with the controller's prior consent, to ensure that the processor's staff are committed to confidentiality and to assist the controller in complying with its data breach notification obligations as well as the rights of individuals.

12. INCREASED PENALTIES

The penalties for non-compliance with the GDPR have been increased. For example, businesses can be fined up to €20 million or 4% of annual global turnover whichever is the greater for offences such as not having sufficient

consent from individuals for processing their personal data or for violation of the basic principles for processing (namely personal data is processed lawfully, fairly and in a transparent manner; is collected for a specified, explicit and legitimate purpose; is adequate, relevant and limited to what is necessary for the purpose; is accurate and kept up to date; is kept for no longer than is necessary; and is kept secure). Businesses can also be fined up to €10 million or 2% of annual global turnover whichever is the greater for offences such as not conducting a DPIA, not having their records in order or not notifying the supervising authority about a breach.

The above penalties apply irrespective of whether businesses are controllers or processors.

13. ABILITY TO APPOINT A LEAD SUPERVISORY AUTHORITY (LSA)

Enforcement of the GDPR is the responsibility of the DPA (in Ireland this is currently the Data Protection Commissioner until it is replaced by the (yet to be established) Data Protection Commission). Each Member State will appoint one or more independent public authorities to be responsible for monitoring the application of the GDPR. Businesses must cooperate with the DPA on request.

Businesses that operate in more than one Member State should appoint the LSA which will have the primary responsibility for dealing with queries and complaints regarding cross-border processing. The LSA must be the DPA in the EU member state where the 'main establishment' of the business is located. Generally, the main establishment is the place of central administration of the business. However if the data protection decision-making occurs elsewhere in the EU, the establishment where such decision-making takes place is the main establishment.

Key actions to comply with the GDPR

Preparation is key to the smooth transition to the new data protection standards. The sooner preparations commence, the easier it will be for businesses to transition to the new standards as it means that they will have time to ensure that they have adequate procedures in place to deal with the improved transparency, security and accountability.

If businesses are compliant with the existing data protection law, this is a good starting point to build on.

However, there are a number of key actions that can be taken, some of which are set out in the following pages.

STEP 1

Carry out a data audit!

Document what personal data you hold, where it came from, why was it originally gathered, how long you will retain it, how secure is it and who you share it with – so that if you hold inaccurate information you will know this and be able to rectify it. You should identify (and document) the basis (under law) for your processing personal data (eg processing is based on consent or processing is necessary to perform a contract) as some individuals rights will be modified depending on your lawful basis for processing their personal data. For example, individuals have a stronger right to have their data deleted where consent is used as the lawful basis for processing.

STEP 2

Review privacy policies

Review your privacy policies in order to address the additional information requirements that are necessary under the GDPR. Information must be provided in concise, easy to understand and clear language.

STEP 3

Review your plan for dealing with access requests

Review procedures to ensure that they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format, if requested. Consider and plan how you will deal with requests from individuals (eg seeking access or deletion of their data). The timescale for processing requests have been shortened from 40 days to one month. If you handle a large volume of access requests, you should consider the logistical implications of having to deal with requests more quickly.

STEP 4

Review how you seek, record and manage consent

Review how you seek, record and manage consent and whether you need to make any changes to this process. You are not required to refresh all existing consents in preparation for the GDPR, but if you rely on consent to process personal data, you should ensure that it meets the GDPR standard on being freely given, specific, informed, unambiguous and in plain language. If not, alter your consent procedures and seek fresh GDPR-compliant consent or find an alternative basis under the GDPR for processing personal data.

STEP 5

Consider children and consent

In relation to children, consider whether you need to put systems in place to verify individuals' ages and to obtain parental / guardian consent for any data processing activity. If you offer online services to children and rely on consent to collect information about them, then you may need consent from a parent / guardian in order to process the child's personal data lawfully. The consent has to be verifiable and your privacy notice must be written in language that children will understand.

STEP 6

Consider if you need to appoint a DPO

Consider whether you need to appoint a DPO. Even if you conclude that you do not need to appoint a DPO under the GDPR, you should still identify a person who is responsible for the organisation's data protection compliance, careful not to designate that person as a DPO which would result in GDPR compliance requirements.

STEP 7

Review and update data breach procedures

Review procedures to ensure that you will be able to detect, report and investigate personal data breaches. You should have an incident response procedure in place in the event of a personal data breach and have a clear plan of action and ensure it is implemented and tested as it will need to be live by 25 May 2018.

STEP 8

Remember your employees and your suppliers

Your employees should be made fully aware of the implication of the changes and should be trained in the application of any new policies. DPIAs may need to be conducted if required and measures should be adopted to mitigate risk.

Review your arrangements with suppliers as it may be necessary to make contractual amendments in order to comply with the GDPR.

STEP 9

Start keeping records of your data processing activities

You will also need to keep a record of data processing activities which must be provided it to the DPA, on request, to demonstrate compliance.

STEP 10

Consider the international element, if necessary

If your business operates in more than one EU Member State, you should map out where your business makes its most significant decisions about its data processing activities. This will help to determine your 'main establishment' and therefore your LSA. This should be documented.


BEAUCHAMPS

THE GDPR JARGON BUSTER:

ARTICLE 29 WORKING PARTY

"Article 29 Working Party" means the advisory body consisting of representatives from EU Member States supervisory authorities together with the European Commission and the European Data Protection Supervisor, which issues guidelines on the implementation and application of EU data protection law. This body will become the 'European Data Protection Board'.

CONSENT

"Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

KEY TERMS:

- Article 29 Working Party
- Consent
- Controller
- Personal Data
- Processing
- Processor
- Personal data breach
- Special categories of personal data
- Supervisory authority

CONTROLLER

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

PERSONAL DATA

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject') such as a name, an identification number, location data or an online identifier.

PROCESSING

"Processing" means anything that is done to or with personal data such as collection, recording, organising, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

PROCESSOR

"Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

PERSONAL DATA BREACH

"Personal data breach" means a security breach which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

SPECIAL CATEGORIES OF PERSONAL DATA

"Special categories of personal data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership as well as genetic data, biometric data, health data or data concerning a natural person's sex life or sexual orientation.

SUPERVISORY AUTHORITY

"Supervisory authority" means an independent public authority which is established by a Member State pursuant to Article 51.

RIVERSIDE TWO
SIR JOHN ROGERSON'S QUAY
DUBLIN 2, D02 KV60, IRELAND

www.beauchamps.ie

BEAUCHAMPS