WOLFE & CO.
— SOLICITORS —
EST. 1894

Market Street
Skibbereen
Co. Cork, P81 W603

Tel: +353 (0)28 21177
Fax: +353 (0)28 21676
E-Mail: info@wolfe.ie
Web: www.wolfe.ie

GENERAL DATA PROTECTION REGULATION ('GDPR')

How is your business weathering the storm?

WHAT IS GDPR?

GDPR is one of the most significant developments in data protection law in decades. The EU regulation came into force in Ireland on 25 May 2018 and replaced the existing data protection framework.

DOES GDPR APPLY TO YOU AND YOUR BUSINESS?

The regulation not only updates how Personal Data may be processed in the digital world, but also seeks to bring about change in terms of how businesses and public bodies treat Personal Data. **GDPR applies to any business (however small) that holds or processes the Personal Data of any EU citizens.**

WHAT IS PERSONAL DATA AND WHO IS THE DATA SUBJECT?

Personal Data means any information relating to an identified or identifiable individual called the Data Subject.

The Data Subject is the individual who can be identified, either directly or indirectly, by reference to Personal Data such as a name, ID number, postal address or online identifier.

The regulation also includes Special Categories of Personal Data which is Personal Data that references either racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data or information concerning health or sex life or sexual orientation.

Special Categories of Personal Data are deemed to be Personal Data of a more sensitive nature and require additional consideration when being processed by the Data Controller and/or Data Processor.

WHO ARE THE DATA CONTROLLER AND THE DATA PROCESSOR?

The Data Controller is the individual or organisation that (either alone or jointly with others) determines the purposes and means of the processing of Personal Data.

The Data Processor is the individual or organisation that processes Personal Data on behalf of the Data Controller.

Note: The definition of 'processing' is very broad and includes but is not limited to any collection, recording, organisation, structuring, storage, adaption, alteration, retrieval, consultation, use, disclosure, erasure or destruction of Personal Data.

SO WHAT HAS CHANGED?

Many of the main concepts and principles of GDPR are much the same as those in the previous Data Protection Acts of 1988 and 2003. However, GDPR seeks to further standardise and strengthen the data privacy rights of EU citizens, while at the same time, emphasising transparency, security and accountability obligations of Data Controllers and Data Processors.

GDPR also introduced certain new obligations and fortified existing provisions relating to security of data, data breaches, requirements to notify breaches to the Data Protection Commissioner ('DPC') and penalties for such breaches.

Some elements of GDPR are more relevant to certain businesses than others, and it is important and useful to identify and map out those areas that will have the greatest impact on your particular business model. Any such review should be implemented as soon as possible to ensure that you have adequate governance and procedures in place.

CAN YOU BE FINED IF YOU ARE NOT GDPR COMPLIANT?

The answer is **YES.** Along with the obvious legal requirements to adhere to the regulation, the earlier you are fully compliant with GDPR the sooner you minimise what could prove to be a costly risk to your business. This is because GDPR gives the DPC more robust powers to tackle non-compliance which include significant monetary penalties.

The level of potential sanction will depend on the breach. Fines range from:

- up to 10,000,000 EUR (or 2% of total annual worldwide turnover in the previous financial year, whichever is greater) for breaches such as non-compliance with the processing related obligations or failure to appoint a Data Protection Officer, where obligatory, to fines of:

- up to 20,000,000 EUR (or 4% of total annual worldwide turnover in the previous financial year, whichever is greater) for the more serious infringements to include breach of the lawful processing requirements or breach of the rights of the Data Subject.

GDPR puts the Data Subject in the driver's seat and makes it considerably easier for individuals to bring private claims against Data Controllers when their data privacy has been infringed. The regulation also provides for Data Subjects who have suffered non-material damage as a result of an infringement to sue for compensation.

SO HOW ARE YOU COPING?

Are You Aware?

You need to be aware that the responsibility to become familiar with the regulation and comply with its provisions lies with you and your organisation. Therefore, if you have not already done so, you need to ensure that certain appropriate organisational, practical and technical security measures exist within your business.

From an organisational perspective, all your employees should already have received a basic training in the general principles of GDPR and should have been made aware of the consequences of failure to apply the rules. They should have an understanding of the types of Personal Data you are processing and what you intend to do with it. You should have easily accessible documented procedures in place to ensure all employees know how to, for example, recognise and respond to a Data Subject access request or to a Personal Data breach.

You should also have appointed a responsible and senior individual who has the knowledge, support and authority to effectively oversee all data protection matters within the business. This is a requirement not to be overlooked or underestimated as it is important to have such an individual who can act as a single point of contact for all other employees, be conscious of training requirements and further nurture a compliant and secure environment.

With regard to practical and technical measures, it is imperative that you have checked your IT and physical surroundings to verify that you are complying with GDPR requirements. This includes password protecting all your computers, using industry standard inscription technologies and systematically destroying, erasing or anonymising Personal Data when it is no longer legally required to be retained. Practically, it also involves simple measures such as keeping all information on computer screens and manual files hidden from callers to your place of business, having access to Personal Data restricted to authorised personal on a 'need to know' basis, keeping paper files in a secure environment and carefully disposing of all waste papers, printouts, etc.

Finally, once you have got your own house in order you should double check that your suppliers and contractors are also GDPR compliant and that you have robust contract terms and confidentiality agreements in place. Where your suppliers (as Data Processors) are processing Personal Data for you (as Data Controller), you will need to have updated your contract with them so they are contractually obliged to provide GDPR compliant data protection standards.

Are You Accountable?

GDPR requires you to demonstrate and document that you understand the types of Personal Data you are holding or processing, where it has come from and what you intend to do with it. This is called the 'accountability principle'. The reasoning behind this measure is to assist with other requirements in GDPR. For example, this inventory will enable you to better manage your library of Personal Data, will facilitate the process of amending inaccuracies or responding to Personal Data

breaches and/or Data Subject access requests in future, where asked to do so and enable you to provide a record of your Personal Data processing to the DPC in a timely manner if so requested.

You should already have created or be in the process of creating a Personal Data inventory which identifies and documents your legal basis for collecting the Personal Data (why you are gathering it in the first place), how you obtained it ('lawfully, fairly and in a transparent manner'), why you are holding it (you should keep it only for one or more specified, explicit and lawful purposes and it should be accurate, complete and up to date), how you will retain it (you should retain it for no longer than is necessary for the purpose or purposes) and if, and on what basis you already have or intend to share it with third parties.

You will also need to identify if the Personal Data has or will ever be transferred outside the European Union ('EU') as there are special conditions that have to be met if transferring Personal Data outside the EU where the importing country does not have an EU approved level data protection).

In certain circumstances, there is an exception to this requirement for entities with less than 250 employees. However, such exception is limited in scope and **does not apply**, for example, where the processing is likely to result in a risk to the rights and freedoms of Data Subjects, where the processing includes any Special Categories of Personal Data or where the processing includes any Personal Data relating to criminal convictions and offences. Further legal guidance should be sought on specific cases.

GDPR also introduced special protections for Personal Data held on children, particularly in the context of social media and commercial internet services. If the child is below the age of 16 years, you must obtain consent from a guardian before processing and consent needs to be verifiable and communicated to the child(ren) in language they can understand.

Remember, the inventory needs to include **past** and **present** records of any Personal Data you continue to hold or process (this is to include all Personal Data held on employees and contractors).

Are You Communicating?

Along with establishing an internal Personal Data inventory, GDPR requires you to give similar information to individuals in advance of processing their Personal Data such as your legal basis for gathering the information, what you intend to do with it, retention periods etc. You also need to inform them of their individual rights under GDPR and the right of complaint where customers are unhappy with your implementation of any of these criteria.

The legal basis for gathering Personal Data includes but is not limited to consent, legitimate interest, contractual necessity, the administration of justice or otherwise. It is important that you document this particularly where consent is relied upon as the sole legal basis for processing the Personal Data.

Consent needs to be 'freely given, specific, informed and unambiguous' and it is imperative to have a documented audit trail to reflect same. Essentially the individual cannot be forced into consent and must be aware that they are consenting to the processing of their Personal Data e.g to receive a newsletter. It is not enough to assume or add a disclaimer and providing an opt-out is not enough. You should also note that individuals must be informed in advance of their right to withdraw their consent at any time.

All such information should be contained in any documentation currently used to communicate about Personal Data e.g. your current data privacy statement on your website, any letters of engagement with a third party, any Data Subject access requests or your employee contracts. You should note that there are extra requirements relating to the form of such notices where the notice is directed to children or vulnerable people.

To comply with GDPR you should have already made a list of all documents and notifications (electronic or otherwise) used to alert individuals to the collection of their Personal Data and updated same to and ensure they are GDPR compliant. If you are relying on consent alone to process Personal Data, you should have a documented process on how you how you seek, obtain and record that consent.

Are You Prepared?

Familiarise yourself with Data Subject access rights and Data Subject access requests

GDPR provides rights called Data Subject access rights which allow individuals, for example, to have access (A Data Subject access request) to their Personal Data (including the categories of Personal Data and your purpose for processing it), to have inaccuracies in their Personal Data corrected, to have information erased ('the right to be forgotten'), to object to direct marketing, to restrict the processing of their information, including automated decision-making and, where applicable, to request Personal Data portability (this right allows individuals, in certain circumstances, to obtain and, more importantly, re-use their Personal Data or require the Data Controller to transfer their Personal Data directly to a third party).

To make a Data Subject access request the Data Subject must apply to you in writing (which can include email) and give any details which might be needed to help you identify the individual and locate all the information you may keep about them e.g. previous addresses, customer account numbers.

The rules for dealing with Data Subject access requests have become more stringent since GDPR was introduced. You are required to provide detailed information when responding and the timescales for complying with such requests have been reduced. Upon receiving a request, you are now required to comply without undue delay which means within one month (with a maximum two month extension depending on complexity and number of requests). Thus, you need to satisfy yourself that you and your employees are in a position to access the information required and deal with the request in a timely manner.

In most cases you will not be able to charge for processing the request (unless you can demonstrate that the cost is excessive) and in most cases you will not be able to refuse to grant an access request unless such a request is deemed manifestly unfounded or excessive. Any information you provide to the Data Subject has to be provided in concise, easy to understand and clear language and you have to provide the information in electronic form where the Data Subject has requested the information by electronic means.

You should note that certain limitations to the Data Subject access rights exist within the legislation and these generally relate to matters of legal privilege or important objectives of general public interest. Further legal guidance should be sought on specific cases.

Familiarise yourself with reporting Personal Data breaches

GDPR has introduced mandatory notifications where there has been a Personal Data breach. This reporting requirement will be new to many businesses. What constitutes a Personal Data breach is broadly defined in the regulation. The concept of breach covers more than an unauthorised use or disclosure of Personal Data.

While the obvious breach events e.g. IT system hack or inadvertent disclosure by employee are included, GDPR also states that any breach of security giving rise to accidental or unlawful destruction, loss or alteration of data, will need to be assessed to determine whether the mandatory breach notification obligations are triggered.

If you have not done so already, you must internally document every Personal Data breach and address the cause in an appropriate and timely manner. Failure to do so may result in a broad range of physical, material and immaterial damage, such a loss of control over personal data, financial loss, identity theft and damage to reputation.

If you are a Data Processor you must notify your Data Controller without undue delay. If you are a Data Controller, you must notify the DPC typically within 72 hours of you becoming aware of the breach 'unless such Personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons'. You must record your reasons for reporting (or not reporting) the breach to the DPC.

Breaches that are likely to result in high risk to the rights and freedoms of natural persons and cause harm to an individual such as identity theft or breach of confidentiality must also be reported to the individuals concerned without undue delay.

You should already have a procedure in place to detect, report and investigate any Personal Data breach. You should verify that your employees recognise what constitutes a Personal Data breach and are aware of the need to report any such breach to the individual responsible for GDPR compliance. Finally, you need to ascertain that you have procedures in place to minimise further potential Personal Data breaches.

It is worth noting that a failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

The value of Personal Data should not be underestimated in our current world. GDPR may create challenges, but it also creates opportunity to build deeper trust and retain clients for those companies who show awareness of their on-going obligations, are transparent about how the data is used and demonstrate that they value an individual's right to privacy.

October 2018 Wolfe & Co. Solicitors
Market Street, Skibbereen, Co. Cork - web: www.wolfe.ie
Tel: 028-21177, fax: 028-21676, e-mail: info@wolfe.ie