In the context of carrying out your business, you will invariably deal with people's personal information on a daily basis. The collection, use and storage of this information is regulated by data protection legislation. It is very important that both you and your staff are aware of data protection law and how to comply with it. While there are already significant penalties for breaches of data protection legislation, the new General Data Protection Regulation (GDPR), which became law on 25 May 2018, significantly increases the penalties that can be imposed and the remedies available to individuals whose data protection rights have been breached. As such, compliance with data protection law is more important than ever.

Many of the main concepts and principles of the GDPR are the same as those set out in our current legislation. The GDPR, however, introduces some new elements and increases some existing obligations for organisations under data protection legislation.

In this guide we take you through the key areas which may impact your business.

**GLOSSARY OF TERMS**

To assist you we have set out below a glossary of some key terms used in this guide.

**Personal Data:** means any information relating to an identified or identifiable natural person (“data subject”). An identifiable person is one who can be identified directly or indirectly, by reference to an identifier such as a name, identification number, location data, online identifier or one or more factors specific to the physical, genetic, mental, economic, cultural or social identity of that natural person.

**Processing:** means any operation or set of operations which are performed on personal data or sets of personal data, such as collection, recording, organisation, storage, adaption, alteration.

**Data Controller:** means the individual or organisation who either alone, or jointly with others, determines the purposes and means of processing of personal data.

**Data Processor:** means an individual or organisation that processes personal data on behalf of the controller.
1. INFORMATION TO BE PROVIDED TO INDIVIDUALS WHEN COLLECTING THEIR PERSONAL DATA

**KEY CHANGE**

The GDPR requires more information to be provided to individuals (data subjects) when their personal data is being collected by the data controller:

In the course of your business you are very likely to collect data about your employees, clients, and potential clients. The GDPR requires that at the time of collecting personal data the following information should be provided by the data controller:

- The identity and contact details of the data controller;
- The contact details of the Data Protection Officer (DPO) (where applicable);
- The purposes of the processing and the legal basis for the processing. Where the processing is based on legitimate interest, what that legitimate interest is;
- The fact that the data may be transferred outside of the European Union (where applicable);
- The recipients or category of recipients of the personal data;
- The period for which the personal data will be stored; or if that is not possible, the criteria used to determine that period;
- The various rights of the data subject, including the right of access, rectification, erasure, restriction of processing, right to object to the processing and the right to data portability;
- Where the processing is based on consent, the right to withdraw consent at any time;
- The right to lodge a complaint with a supervisory authority;
- Whether provision of the personal data is a statutory or contractual requirement and, the consequences of failing to provide that data;
- The existence of automated decision-making, including profiling, and information on the logic involved and the consequences of such processing for the data subject.

**ACTION**

In order to comply with this new requirement, you should update all information and privacy notices used when personal data is collected.
2. CONSENT

There are a number of grounds upon which organisations can rely to process and/or use people’s data. These include:

- Where the individual has consented to that processing;
- Where the processing is necessary for the performance of the contract which the individual is a party to;
- Where the processing is necessary for compliance with a legal obligation which the organisation may be subject to.

Where you are relying on consent to process somebody’s personal data you will need to be aware of the new rules in relation to consent.

Under previous data protection legislation, consent could be explicit or implied. The GDPR however requires a higher threshold for the collection of consent. Consent must now be freely given, specific, informed and unambiguous. Silence and inactivity can no longer be relied upon. An individual now has a right to withdraw his or her consent to the processing at any time. Prior to giving consent the individual must be informed of this right to withdraw.

**KEY CHANGE**

Where you rely on consent as a ground to process personal data, which you are likely to do in a number of circumstances (e.g. contacting individuals for client satisfaction surveys) you will need to ensure that you comply with these conditions in relation to consent. This includes informing the individual of their right to withdraw consent. You will now need to review the ways in which you obtain consent and where necessary review your consent forms. Where consent was not obtained in compliance with the GDPR, you may not be able to rely on it post 25 May 2018 and it may be necessary to obtain consent again.

**ACTION**

Where you rely on consent as a ground to process personal data, which you are likely to do in a number of circumstances (e.g. contacting individuals for client satisfaction surveys) you will need to ensure that you comply with these conditions in relation to consent. This includes informing the individual of their right to withdraw consent. You will now need to review the ways in which you obtain consent and where necessary review your consent forms. Where consent was not obtained in compliance with the GDPR, you may not be able to rely on it post 25 May 2018 and it may be necessary to obtain consent again.
3. DATA BREACHES

**KEY CHANGE**
Under our current system of data protection legislation there is no mandatory requirement to report a data breach to the Data Protection Commissioner. The GDPR, however, requires that all data breaches must be reported to the Data Protection Commissioner within 72 hours, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the personal data breach is likely to result in a high risk to the rights and freedoms of the individual concerned, then the breach should also be notified to that individual without delay.

**ACTION**
You should ensure that your data protection policy is updated to reflect this requirement and that your staff are aware of it.

4. ENGAGING DATA PROCESSORS

**KEY CHANGE**
You may, in certain circumstances, engage a third party organisation to process data on your behalf (data processors). For example, if you engage the services of a marketing company or CRM company to run a marketing campaign on your behalf; or where you engage a payroll company to carry out your staff payroll. You are required to have a written authorisation in place which contains certain mandatory clauses with such data processors. The GDPR requires that additional clauses be included in such a written authorisation.

**ACTION**
You should review the organisations which you engage to process data, ensure that there is a written contract in place regulating the processing of data and seek to update this contract with the relevant clauses required by the GDPR.
5. DATA PROTECTION OFFICER

**KEY CHANGE** The GDPR requires that organisations designate a DPO in certain circumstances, including where the core activities of the controller or processor consist of processing operations which by virtue of their nature, scope and purpose, require regular and systematic monitoring of data subjects on a large scale or where the core activities of the controller or processor consist of processing of special categories of data, such as data concerning health, or personal data relating to criminal convictions and offences.

**ACTION** You will need to consider whether or not your organisation is required to appoint a DPO. If it is, you will need to identify who the relevant individual should be. This individual can either be employed by the organisation or be a consultant to the organisation. Where the DPO is employed by the organisation, he or she may fulfil other tasks and duties but those tasks and duties should not result in a conflict of interest with their function as a DPO.

6. INCREASED PENALTIES

**KEY CHANGE** There has been a significant increase in the penalties which can be imposed upon organisations for failing to comply with their obligations under the GDPR. The maximum fines which can now be imposed are €20,000,000 or 4% of worldwide annual turnover, whichever is the larger.

In addition, an individual whose data rights are breached can take a claim against the organisation that breached their rights for both material and non-material damage. Under previous data protection legislation, individuals could only bring a claim for material damage (i.e. out of pocket expenses or actual damage) as opposed to non-material damage.

Given the increased penalties and the risk of compensation to individuals in the event of their data protection rights being breached, a breach of data protection legislation is a real financial risk to your organisation. As such you should ensure that both you and all of your staff are fully aware of and compliant with data protection legislation.
SOME KEY STEPS IN ORDER TO COMPLY WITH THE GDPR

- Review the personal data that you collect and review the ways in which this data is processed. Review the legal ground upon which you rely to process this data. You should ensure that all data is processed in accordance with the relevant legal grounds that are set out in the GDPR.

- Update privacy notices at the point of collection of the data so that they comply with the GDPR.

- Consider what organisations you engage to process data on your behalf and check whether there is a contract in place with them. If not, put one in place and check whether any existing contracts need to be updated to include the necessary mandatory terms.

- Begin to train yourself and your employees on changes brought about by the GDPR.

- Update your data protection policy to take account of the GDPR.

- Consider whether you need to appoint a DPO.

This guide sets out a summary of some of the key changes brought about by the GDPR. The GDPR does bring about many more changes to data protection legislation. For more information please contact a member of our team.