**What is GDPR?**

GDPR stands for the General Data Protection Regulation and UK’s framework for data protection laws. GDPR It came into effect in the UK on 25th May 2018, even though it is EU regulation, it has been incorporated into the UK data protection law at the end of the Brexit transition period.

The GDPR seeks to strengthen the protection of personal data by making good data protection practice and governance an integral part of business. It provides individuals with new, stronger rights and protections and also provides supervisory authorities with new powers including the ability to audit, suspend or ban processing and impose financial penalties. Within the GDPR there are large changes for the public as well as businesses and bodies that handle personal information.

In a nutshell, under the GDPR, there are new rights for people to access the information companies hold about them, obligations for better data management for businesses, and a new regime of fines. GDPR intends to give individuals control over their private data and is based on seven principles of: lawfulness, fairness and transparency; purpose limitation; integrity and confidentiality; data minimisation; storage minimisation; data accuracy and accountability.

**Who does the GDPR apply to?**

The legislation applies to every business large and small in the UK including charities - there will be no exceptions for small businesses.

Not everyone that handles the personal data of individuals is the same and data protection laws allow for this by having two different terms: controller and processor.

A controller is an entity that decides the purpose and manner that personal data is used, or will be used.

A processor is responsible for processing personal data on behalf of a controller.

If you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.

The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

**What is personal data under the GDPR?**

Personal data can be anything that allows a living person to be directly or indirectly identified. This may be a name, an address, biometric data or even an IP address. It includes automated personal data and can also encompass pseudonymised data if a person can be identified from it.

**What is sensitive personal data under the GDPR?**

GDPR calls sensitive personal data as being in 'special categories' of information. These include trade union membership, religious beliefs, political opinions, racial information, and sexual orientation.

**What is considered processing data under the GDPR?**

“Processing” means doing any of the following with personal data: obtaining it; recording it; storing it; updating it; sharing it. “Personal information” means any detail about a living individual that can be used on its own, or with other data, to identify them.

**Processing personal data under GDPR in a nutshell**

* You must have a valid lawful basis in order to process personal data.
* There are 6 available lawful bases for processing. No single basis is ’better’ or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.
* Most lawful bases require that processing is ‘necessary’. If you can reasonably achieve the same purpose without the processing, you won’t have a lawful basis.
* You must determine your lawful basis ***before*** you begin processing, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason.
* Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.
* If your purposes for processing change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).
* If you are processing special category data, you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
* If you are processing criminal conviction data or data about offences, you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

**What are the lawful bases for processing under the GDPR?**

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

1. **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
2. **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.
3. **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
4. **Vital interests:** the processing is necessary to protect someone’s life.
5. **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.
6. **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.)

**Data processing principles under the GDPR**

When processing personal data all businesses and organisations must follow the following six principles. Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

**Rights for individuals under the GDPR**

* 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.

**Proof of Compliance**

Businesses should keep a record of how they are securely protecting the data that they process and manage. Should your business be subject to an audit or a GDPR breach, you will need to show evidence that demonstrates that you have taken the appropriate actions to protect personal data held by your organisation and any third party organisations.

**Dealing with a data breach under GDPR**

Businesses must issue notifications of valid data breaches to the local supervisory authority within 72 hours of becoming aware of them. Failing to report a breach can result in an investigation and/or penalties. Individuals also have the option to file a class action lawsuit if a business does not comply with GDPR.

There is a mandatory breach reporting requirement, where employers must report certain types of breaches to the data protection authority. A personal breach occurs where a business’s security systems have been compromised leading to the ‘accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data’.

A business must determine the level of the breach’s severity and the risk it could present to an individual’s rights and freedoms. If it is considered a risk, then you must notify the Information Commissioner’s Office (ICO). If there is no risk, then you do not have to report it. However, businesses who do not report a breach should keep a record and be able to justify their reasoning behind their decision not to report it and document those reasons.

Businesses should have suitable procedures in place to notify the regulator where breaches have been reported and identified. Inform all staff of the correct procedure to follow should a breach occur.

**Why should businesses bother with compliance?**

* **Fines & Penalties:** There are risks of fines by the Information Commissioner’s Office (supervisory authority), depending on the category of the data breach, of up to €20 million (or 4% gross annual global turnover, whichever is greater). Having said this, beware of scaremongering – the ICO isn’t on the war path to fine everyone with a minor breach. They may make suggestions to enable companies to become compliant in some cases where they decide not to impose fines.
* **Compensation claims:** Individuals can also take organisations to court for compensation if they feel their rights have been breached.
* **Reputational damage:** The ICO will look to make examples out of organisations not conforming to GDPR or taking action. The media will be reporting about businesses with data breaches as the latest ‘hot topic’.

**Steps to compliance**

1. Identify what personal data you process. This can be achieved by carrying out a data mapping exercise/data audit.
2. Review the processing activities that you carry out and where necessary:
* identify your purposes for processing personal data;
* whether the personal data you process includes any special categories of personal data;
* identify the lawful basis for all processing of personal data (remember, there are 6 lawful bases);
* ensure that you are only processing the minimum amount of personal data necessary for the identified purpose;
* ascertain how you confirm that the personal data obtained is accurate and where necessary ensure there are processes in place to keep that data accurate; and
* establish and justify the periods for retaining that data
1. Determine how you will provide information to the various data subjects, including staff, volunteers, customers, members, etc which explains why you need to process their personal data, what you will use that data for, including who it may be disclosed to, and how long you will keep that data.
2. Implement appropriate technical and organisational measures to ensure personal data (whether held electronically or on paper) is securely stored and safely destroyed or deleted when no longer required.
3. Ensure there are processes in place to facilitate requests from data subjects seeking to exercise their rights.
4. Where appropriate, have up-to-date policy/procedure documents that detail how your business or organisation is meeting its data protection obligations.
5. The GDPR introduces a duty for you to appoint a data protection officer (DPO) if you are a public authority, or if you carry out certain types of processing activities. Determine whether you require a Data Protection Officer (DPO).