An overview of the GDPR

In a nutshell

The *General Data Protection Regulation* is a new law applying directly across the European Union from 25 May 2018. It will continue to apply in the UK even after Brexit.

There is a fair amount in the GDPR that is not new. However, it extends the rights to individuals in relation to data protection; and places significant transparency and accountability requirements on organisations. The regulatory body in the UK will be the Information Commissioner's Office (ICO); and fines for a breach of the GDPR can be up to 4% of global annual turnover or €20 million, whichever is greater.

Provisions

The GDPR is based on six data principles; and anyone using personal data must have a prescribed lawful basis for doing so. It also provides for special categories of data; for a wide range of individual rights; and for rules regarding transparency and accountability. Data controllers will no longer need to register with the ICO under the GDPR, but unless they are exempt, they will have to pay a data protection fee.

What is personal data?

Personal data is anything from which a person can be identified. It includes identity numbers, payroll numbers, biometric data or any other category of data from which points to an identifiable individual. It does not include data processing carried out by individuals purely for personal/household purposes.

Special categories

Under GDPR, what was previously called sensitive data such as sex, race, religion, health, union membership etc. is now known as special category data. It includes biometric data (where used for ID purposes) but excludes criminal conviction data. To process this type of data you need a "condition" as well as a lawful basis for your processing. These extra conditions have been clarified by the new *Data Protection Act 2018*, which took effect at the same time as GDPR, and a full list can be found schedule 1 of the Act.

Processing criminal conviction data is separate to that for special category data, but still requires a condition plus a lawful basis (again, see schedule 1 of the *Data Protection Act 2018*).

The six data principles

These state that personal data must be handled as follows:

- Processed lawfully, fairly and transparently
- Collected for specified, explicit and legitimate purpose
- Adequate, relevant and limited to what is necessary
- Accurate and kept up-to-date
- Kept for no longer than necessary
- Processed in a secure manner

A lawful basis for processing

The processing of personal data may only be carried out if one or more of the following lawful basis can be applied to the specific processing operation:

Consent: To apply, consent must be freely given, specific, informed and unambiguous. So ready-ticked boxes, bundled up purposes for consent, and opt-out scenarios are not acceptable. Also, individuals must be told of their right to, and be able to, withdraw their consent.

Contractual: This can apply to data needed to fulfil a contractual obligation, or to take pre-contractual steps. The processing must be necessary to deliver your side of the contract; and not be undertaken off your own back.

Legal obligation: This applies where the processing of personal data is required to comply with common or statute law. (It specifically excludes contractual obligations which are covered above).

Vital interest: This can apply if processing is required to protect a person's life, even if the person at risk is not the data subject. It does not apply however if the data subject is capable of giving consent. It is most likely to be used in emergency situations.

Public interest: This applies to processing of personal data in order to perform a statutory task in the public interest, or to perform official functions. It will apply mostly to public authorities.

Legitimate interest: This somewhat vague and flexible basis might apply if processing is carried out in a way people would reasonably expect and has a minimal impact on privacy; or where there is a compelling justification. The processing must be a targeted and proportionate way of achieving your purpose, and you must balance your interests against those of the data subject. The ICO recommend you undertake a legitimate interest assessment before using this as your lawful basis for processing. This is a 3-part test to check (1) that your purpose is a valid legitimate interest; (2) that it is necessary; and (3) that individual rights and freedoms are not overridden.

The rights of individuals

A key part of GDPR is strengthening the rights of individual. These can be summarised as *a right*:

To be informed: The GDPR sets out what information must be supplied to individuals regarding the use of their data. Some of this will be covered by your privacy notice.

To have access: This allows individuals access to the data you hold on them. It is similar to the existing right, although access requests will be free of charge unless manifestly unreasonable or excessive.

To have errors rectified: You will have to correct errors when notified by an individual, and also inform any third party with whom you shared the data.

To be forgotten: Also known as a right to erasure, this enables an individual to request the removal of data where there is no compelling reason for its continued processing.

To restrict: In certain circumstances, individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, you are permitted to store the personal data, but not further process it.

To portability: This allows an individual to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. It only applies to personal data an individual has provided to a controller; where the processing is based on the individual's consent or for the performance of a contract; and when processing is carried out by automated means.

To object: Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

In most cases, organisations will have up to one month only in order to take action when an individual seeks to enforce their rights.

Transparency: the provision of information

When collecting and using data you must explain what, why and how you are conducting your processing (e.g. through your privacy notice). This also includes information about third parties with whom any data is shared. The GDPR lists a lengthy range of specific details that you are required to provide. Such information must be timely, clear, accessible and provided using plain language.

Accountability

It is inherent in the GDPR data principles that data protection must be built into processing activities. It is referred to as data protection by design. Depending upon the size of your organisation and nature of your data processing you may need to:

- Keep detailed records of processing operations
- Perform data protection impact assessments (DPIA)
- Designate a Data Protection Officer

You will need to ensure that data capture forms, privacy notices, other policies and procedures are all GDPR compliant.

In any event, you must be able to demonstrate compliance, so whether or not you process special categories of data, or meet the criteria of a large employer (250 or more staff), documentation and records will likely be needed in order to evidence your compliance. This will include being able to record and notify data breaches to the ICO (and possibly Charity Commission/Fundraising Regulator where applicable).

Further reading and resources

Your go-to source of detailed information on the GDPR should be the Information Commissioner's Office (ICO). The ICO website has detailed guidance on the GDPR, including checklists, information on privacy notices, direct marketing, and on best practice when obtaining and using consent: https://ico.org.uk/

On the Green Pepper website you will find a GDPR getting ready checklist, a data audit form, a privacy notices checklist, and briefings on consent, legitimate interest, processing special categories of data and using children's personal data. You will also find links to information from other organisations including the Institute of Fundraisers. https://greenpepperconsulting.co.uk/