Interlink

Your local county voluntary council

2. Running your organisation

2.12 Data protection & GDPR

What is the General Data Protection Regulation (GDPR)?

It's a European law that has been introduced to strengthen and unify data protection for individuals within the EU.
Currently, the UK is required to comply with the Data Protection Act 1998 (and the 1995 EU Data Protection Directive), but from 25th May 2018 all EU member states will need to comply with the GDPR instead.
The Information Commissioner's Office (ICO) will regulate the implementation of the GDPR in the UK.

What type of information does the GDPR apply to?

Like the Data Protection Act 1998 (DPA), the GDPR applies to 'personal data', but the definition for that has been expanded. Under the GDPR, personal data means any information relating to an identifiable living person who can be directly *or indirectly* identified from that information.

It also applies to sensitive personal data, which it refers to as 'special category data'. Those categories are subject to additional protections, and include data that relates to an individual's race or ethnic origin, religion, health, and genetics. Biometrics are also now included if that data is used to uniquely identify an individual. Data relating to criminal convictions or offences is not classed as special category data, but there are separate safeguards in place for this type of data within Article 10 of the GDPR.

Will I need to comply with it?

If you work or volunteer for an organisation or business that processes personal data, then it is likely you will need to comply with the GDPR.
It doesn't matter whether you're based within an EU member state or not: if your organisation processes personal data relating to EU residents, and it is classed as either being a 'data controller' or a 'data processor', your organisation will be required to be GDPR compliant.

A data controller is the organisation or person (such as a sole trader) that collects and uses personal data, and determines the purposes and means of processing that data.
A data processor is the organisation or person that is responsible for processing personal data on behalf of a data controller. This might include organisations providing services such as payroll management, mail delivery, IT systems, and confidential

waste disposal. The GDPR places specific legal obligations on data processors which have not been in place under the DPA, and processors will now have legal liability if they are responsible for a data breach.

How is the GDPR different to the DPA?

There are many similarities between the two pieces of legislation, but the GDPR has introduced a number of new provisions that you will need to be aware of.

Principles

The number of data protection principles has been reduced from 8 to 6, but they do remain very similar in content to the 8 principles set out in the DPA. The 6 principles of data protection that are now set out under the GDPR state that 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 processed in any 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;
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;
6. processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures.

The GDPR also sets out an overarching principle of accountability. This requires data controllers to be responsible for, and be able to demonstrate compliance with, the 6 principles set out above.

Privacy notices

A privacy notice is a statement that you provide to individuals when you collect information from them, setting out what they need to know regarding data protection. The GDPR introduces a requirement for more detailed privacy notices to be provided to individuals when personal data is collected, including information such as:

- the purpose(s) that the personal data will be processed for
- the lawful basis that the organisation is relying upon to process that individual's data (see below)
- how long the data will be retained for
- who the data will or might be shared with, and
- the individual's right to withdraw consent if they wish to.

Further detail on the information that you need to provide to individuals can be found on the ICO's website.

Data Protection Officers

Under the GDPR, your organisation will need to legally appoint a Data Protection Officer (DPO) if you meet the following criteria:

- you are a public authority;

- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

If you don't meet these criteria, you can voluntarily appoint a DPO if you wish, but you should be aware that the same requirements of the position and tasks apply as they would if the appointment of the DPO was mandatory. Alternatively you can appoint someone to be your organisation's data protection 'lead' (or similar), so that they co-ordinate data protection provisions within your organisation, and possibly act as the person to which staff and/or volunteers report any breaches of data, but they won't have to meet the official requirements associated with the DPO role.
Additional information on the criteria and the specifics of the DPO role can be found in the ICO's Guide to the GDPR, and in this FAQ document.

Enhanced rights

The DPA provides individuals with a variety of rights in relation to their personal data, but those rights will be enhanced by the GDPR, and will include a new right of data portability. The following rights for individuals are set out within the GDPR:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure (also known as the right to be forgotten)
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Full details of each of those rights can be found on the ICO's website.

Lawful basis for processing data

Before you can process any personal data, the GDPR requires you to identify a valid lawful basis for being able to process it. There are 6 bases that you can choose to rely upon, and you will need to determine which one or more of them applies to your data processing activities. The ICO's lawful basis interactive guidance tool can help you with this.

The 6 lawful bases that are available for processing data are:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose (see below for more detail)

(b) Contract: the processing is necessary for a contract that you have with the individual, or because they have asked you to take specific steps before entering into a contract

(c) Legal obligation: the processing is necessary for you to comply with the law (but this does not include contractual obligations that you may have)

(d) Vital interests: the processing is necessary to protect someone's life.

(e) 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 (this is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest)

(f) Legitimate interests: the processing is necessary for your organisation's 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.

Consent

Under the DPA, if you are relying on consent to process an individual's personal data, in most circumstances you can rely on either express consent (where the individual opts in to you using their data in specific ways), or implied consent (where the individual doesn't opt out of you using their data).

If you wish to rely on consent as the lawful basis to process personal data once the GDPR comes in to force, you will no longer be able to rely upon implied consent. It will have to be 'opt-in' consent, which is freely given, specific and informed. This means the threshold for consent is higher under the GDPR, so you might need to alter the way in which you gain consent from individuals (*if* consent is needed for you to process their data), and/or you might need to gain renewed consent from individuals if the consent you currently hold won't be deemed to be GDPR compliant.

The ICO have published guidance on consent, which confirms exactly what criteria needs to be met for consent to be valid under the GDPR. Please note, however, that consent is only one of the 6 options that you have for processing personal data, and it might be more appropriate and/or practical for you to rely on a different lawful basis to process the data instead.

Reporting breaches

Under the DPA, there was no legal obligation for data controllers to report breaches of security, but the GDPR introduces a duty on *all* organisations to report a personal data breach to the ICO *if* they believe it is likely to risk the rights and freedoms of the individual(s) whose data has been breached.

If the organisation believes that such a risk is likely, they will need to report it to the ICO within 72 hours of becoming aware of the breach (if feasible to do so). And if the breach is likely to result in a *high* risk to the rights and freedoms of the individual(s) whose data has been breached, the organisation will also need to inform those individuals of the breach without undue delay.

From a practical perspective, this means that all of the your staff and/or volunteers need to be able to identify a breach if one occurs, and they also need to know who to report such a breach to immediately, so that a report can be filed with the ICO within 72 hours if that is necessary. Most data breaches can be prevented by having robust security measures in place throughout your organisation.

Further information on data breaches and security can be found on the ICO's website.

Data Protection Impact Assessments (DPIAs)

For some time, the ICO has been encouraging data controllers to carry out DPIAs as good practice when working on projects involving personal data. Essentially a DPIA is a process to analyse your data processing, and help you identify and minimise data protection risks. The GDPR will make it mandatory for DPIAs to be carried out for certain types of data processing, or if the processing of an individual's data is likely to result in a high risk to that individual's interests.

The ICO has stated that this is a key element of the new focus that there is on accountability and 'data protection by design' under the GDPR, along with a more risk-based approach to compliance.

Detailed information on how to carry out a DPIA (if you need to) can be found in the ICO's Guide to GDPR, along with a number of checklists that you might find useful.

Fines

Under the DPA, the ICO have the power to impose fines of up to £500,000 for breaches of personal data. The GDPR introduces an increase in the level of those fines, and the maximum penalty could be up to €20 million (approximately £17m) or 4% of global turnover (whichever is larger). The ICO have, however, confirmed that they will only impose fines as a matter of last resort, as they do now. Along with the power to issue higher fines if they feel that is necessary, the ICO will continue to be able to issue other sanctions including warnings, reprimands and corrective orders.

What can I do to ensure my organisation is compliant with the GDPR?

There are a number of practical steps that you can take to try and ensure your organisation will be compliant with the GDPR, from 25 May 2018 and in the future, including:

- Carry out an audit to identify what personal data you hold and what you do with it, and then conduct risk assessments relating to that data so that you can put

measures in place to manage any risks that you identify. The ICO have a number of documentation templates and checklists that you might find useful

- Determine whether your organisation is a data controller or a data processor (or both), and review any written agreements that you have with place with data controllers or data processors to ensure they reflect the new provisions within the GDPR
- If you are relying on consent to process personal data of any individuals, check whether it meets the higher threshold under the GDPR
- Review your privacy notices and ensure they contain the extra detail that the GDPR states is required
- Train staff, volunteers and temps in data protection, and implement policies and procedures throughout your organisation to ensure data is processed in line with the data protection principles
- Determine whether you need to appoint a DPO; and
- Have systems in place to identify and report breaches to the ICO, when necessary.

Further information

Information Commissioner's Office (ICO)
Tel: 0303 123 1113
www.ico.org.uk

This information sheet was produced by Anna Bezodis Training and Consultancy: www.annabezodis.com

For further information contact

Cyngor Gweithredu Gwirfoddol Cymru
wcva
Wales Council for Voluntary Action

Tel: 0300 111 0124
www.wcva.org.uk

Interlink