Swansea Canal Society

Cymdeithas Camlas Abertawe

Data Protection & GDPR Policy

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. Previously, the UK was 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 GDPR instead.

A definition of GDPR is:

Personal data means any information relating to an identifiable living person who can be directly or indirectly identified from that information.

Like the Data Protection Act 1998 (DPA), the GDPR applies to personal data, but the definition for that has been expanded. It also applies to sensitive personal data, which it refers to as 'special category data'. These categories are subject to additional protections, and include data that relates to an individual's race or ethnic origin, religion, health, genetics. Biometrics are also now included if that data is used to uniquely identify an individual.

Data relating to Criminal convictions or offences are not classed as special category data.

When working for a voluntary organisation that processes personal data, then you will need to comply with the GDPR.

A data controller collects and uses personal data and determines the purposes and means of processing that data.

A data processor is responsible for processing personal data on behalf of the controller. This might include provision of services, such as payroll management, mail delivery, IT systems and confidential disposal.

The GDPR places specific legal obligations on the 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.

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 six principles of data protection that are now set out under 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 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 six principles.

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:

1. the purposes that the personal data will be processed for
2. The lawful basis that the society is relying upon to process that individual's data
3. How long the data will be retained for
4. Who the data will or might be shared with, and
5. The individual's right to withdraw consent if they wish to.

Appointing a Data Protection Officer.

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 as data protection lead. They co-ordinate data protection provisions, and as the person any beaches of data are reported to, don't have to meet the official requirements associated with the DPO role.

Enhanced Rights

DPA provides individuals with a variety of rights in relation to their personal data, but those rights will be enhanced by 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 to 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.

Lawful Basis for Processing Data

Before processing any personal data, the GDPR requires you to identify a valid lawful basis for being able to process it. There are six bases that you can choose to rely upon, and you need to determine which one or more of them applies to data processing activities.

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

- Consent: the individual has given clear consent for you to process their personal data for specific purposes
- 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.
- Legal obligation: the processing is necessary for you to comply with the law.
- Vital interests: the processing is necessary to protect someone's life.
- 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.
- Legitimate interests: the processing is necessary for the society'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 GDPR, if you are relying on consent to process an individual's personal data, in all circumstances you can rely on expressed consent (where the individual opts in to you using data in specific ways).

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.

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 Information Commissioner's Office 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). If the breach is likely to result in a 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 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 filled 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.

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.

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 £17 million 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. ICO can issue sanctions including warnings, reprimands and corrective orders.

How to ensure my organisation is compliant with the GDPR

1. Carry out an audit to identify what personal data we hold and what we do with it, and then conduct risk assessments relating to that data so that we can put measures in place to manage any risks that we identify.
2. Determine whether our organisation is a data controller or a data processor (or both), and review any written agreements that we have with data controllers or data processors to ensure they reflect the new provisions within the GDPR.
3. If we are relying on consent to process personal data of any individuals, check whether it meets the higher threshold under the GDPR.
4. Review our privacy notices and ensure they contain the extra detail that the GDPR states is required.
5. Train staff, volunteers in data protection, and implement policies and procedures throughout our organisation to ensure data is processed in line with the data protection principles.
6. Determine whether we need to appoint a DPO.
7. Have systems in place to identify and report breaches to the ICO, when necessary.

External link

The following documents are available on the ICO website:

www.ico.org.uk Tel: 0303 123 1113

Information Commissioner's Office (ICO) GDPR Guide

ICO Lawful basis interactive guidance tool

ICO Guidance on consent

ICO data breaches and Security

Detailed information on how to carry out a DPIA