GDPR

General Data Protection Regulation

Get Ready For Change
- Data Protection

Staff Guide

Clackmannanshire Council | Comhairle Siorrachd Chlach Mhanann
www.clacks.gov.uk

GDPR

How to use this guide

The General Data Protection Regulation (GDPR) comes into force on 25 May 2018. It marks a change for Data Protection legislation so we've prepared this guide to help you navigate it.

Introduction to GDPR

Why is data protection changing?

The first law was introduced in 1984. This was relatively simple in terms of scope and only related to certain types of records, mostly electronic. It was replaced in 1998 by the current Data Protection Act.

The Data Protection Act 1998 provides a more comprehensive framework through which organisations can manage personal data. It provides certain rights to individuals, and protects both people and organisations from potential misuse. However, this law was brought into force before the Internet exploded and does not reflect many of the practices now deemed common place amongst global businesses.

The General Data Protection Regulation (GDPR) has been created to provide more appropriate protections for personal data in the digital age. Although many aspects stay the same, it places some new responsibilities on organisations particularly in relation to how personal data is used, individual rights, and demonstrating compliance.

The New Data Protection Act

The UK government is also currently drafting legislation which promises to adopt the principles of GDPR.

GDPR

What does this mean for the Council

The new privacy framework places a greater focus on accountability which means, in addition to being compliant with data protection principles, the Council will have a duty to document what we do with personal data. This will include having a register of all processing, documenting policies and procedures, and ensuring there are appropriate records in relation to information sharing practices, privacy impact assessments and breach management.

How big is the change?

The new Data Protection Act represents a maturity of existing data protection legislation so many elements will stay the same. The new Data Protection Act continues to have:

- definitions for personal data and sensitive personal data (now known as 'special categories' of data)
- data protection principles which set the framework for how personal data must be handled by organisations
- defined conditions which allow personal data to be processed
- a regulating authority. For the UK, this is the Information Commissioner (www.ico.org.uk)
- specific rights granted to data subjects in relation to accessing data and preventing certain processing
- enforcement powers, including the ability to issue fines
- privacy notices which inform data subjects how their personal data will be used
- processes in place to manage breaches
- information sharing agreements to support processes when personal data is shared with other organisations
- processes which allow the impact on people's privacy to be assessed when new ways of working are introduced or re-designed. These have been known as Privacy Impact Assessments (PIAs) but will be called Data Protection Impact Assessments (DPIAs) under the new Data Protection Act

Is anything new?

The new Data Protection Act introduces a new requirement for all public authorities to appoint a Data Protection Officer. This person will advise senior management about whether we're meeting our responsibilities under the Act and/or the risks associated with carrying out certain actions/processes.

We will also need to produce a Register of Processing. This will document all the occasions when personal data is collected or used by us, and include why it's needed, what happens to it and how long it is kept.

The new Data Protection Act also introduces some new rights for individuals. These are discussed in more detail later but, specifically, there are new rules to govern how children's data should be used. There will also be occasions when individuals can ask for their personal data to be deleted or transferred to another data controller.

Under the new legislation, organisations which process personal data on the Council's behalf will also be liable if the data is breached. This fact will need to be built into contract arrangements in future.

Data Protection Principles

The new Data Protection Act provides a governance framework which is based on six principles. These guide organisations in how they collect and use personal data. The six principles relate to:

Lawfulness, fairness and transparency

Organisations should only process personal data lawfully and in a fair way. We must tell people very clearly what we intend to do with the personal data we collect about them.

Purpose Limitation

Personal data should be collected for specific, explicit and legitimate purposes. If we have collected personal data, and told the individual what we will do with it, we can't use the information for another purpose simply because we hold it.

Data Minimisation

Collected personal data should be adequate, relevant and limited to what is needed. We should only collect the personal data that is required for the task.

Accuracy

Personal data must be accurate and, where necessary, kept up to date. Reasonable steps should be taken to rectify any data that is found to be inaccurate. Any personal data we hold should be routinely reviewed to ensure it is accurate.

Storage Limitation

Personal data should not be kept in a form which allows individuals to be identified for any longer than is necessary for the purpose for which it was collected. Our systems and processes should be designed to delete personal data as soon as it is no longer needed. This might mean that parts of records are deleted at different times.

Integrity and Confidentiality

Personal data should be protected against unauthorised access, accidental loss, destruction or damage. Both physical and technical controls should be used as appropriate.

Data protection principles apply to records capturing personal data in all formats e.g. hardcopy paper, electronic systems, CCTV.

GDPR

Definitions of personal data

What is personal data and when can I use it?

Under the new Data Protection Act 'Personal data' means:

> any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Certain types of personal data need added protection and can only be processed if certain conditions apply. Special category data is personal data which reveals:

> Racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

When can I process personal data?

We can process personal data if it is necessary:

- for the performance of a contract, for example if it's in accordance with a tenancy agreement, or as part of a contracted service
- to enable the Council to comply with a legal obligation like when we need to refer an individual to a regulatory body, process planning or licensing applications, or to collect Council tax
- to protect someone's vital interest: such as responding to child protection concerns
- for the performance of a task which is carried out by the Council in the public interest or in its official authority. This is likely to cover processing required to deliver Council services like social work, education, providing housing, and collecting Council tax

These are known as 'conditions of processing'.

As a public authority, we can't rely on consent as a condition to allow processing of personal data under the new Data Protection Act. This is because consent must be 'freely given' and, as a local authority and employer, we are considered to have an unfair balance of power over individuals.

When can I process special category data?

The conditions which will allow special category data to be processed are different. This information can only be used if it is necessary, to:

- carry out a specific obligation or exercise a right in the field of employment, social security, and social protection law, for example: to provide appropriate pensions
- protect someone's vital interest. E.g. to respond to child protection concerns. (Remember 'vital interest' normally has to relate to potential life or death scenarios)
- establish, exercise or defend legal claims

And for:

- the purposes of preventative of occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment of the management of health or social care systems and services. E.g. to provide occupational health services, or deliver health and social care services
- reasons of public interest in the area of public health
- archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with law
- the personal data has been made public by the data subject

GDPR

Privacy By Design and Data

Data Protection Impact Assessments

We currently conduct Privacy Impact Assessments (PIA) when systems or processes which handle personal data are changed or introduced. Under the new Data Protection Act, these are called Data Protection Impact Assessments (DPIAs) and will become mandatory. The new Data Protection Act requires organisations to adopt 'Privacy by Design', this means that new processes and systems must be designed to ensure that personal data is only processed when necessary and personal data is deleted as soon as possible.

A DPIA may relate to large scale processing such as the introduction of a Council wide case management system, or smaller scale processing like the introduction of a new form or app which collects personal data.

There are various controls which will need to be considered. These will include identifying the minimum amount of personal data required, managing access, providing appropriate security, ensuring that data subjects know what will happen to their data, and deleting it or using anonymisation techniques when it is no longer required.

Data Protection Impact Assessments (DPIAs) provide evidence that we have considered data protection principles when designing processes that handle personal data. They document that we've tried to do the right thing. Under the new Data Protection Act, DPIAs which relate to high risk processes will need to be authorised by the ICO.

Transparency and Openness - Privacy Notices

Privacy notices ensure that people understand why we need their personal data, and how it will be used. Providing clear information about this ensures that individuals are not surprised, and don't feel that their data has been used inappropriately.

Privacy notices need to be clear, easily available, and concise. They must inform individuals of:

- who the data controller is and who in the council to contact for any queries (the Data Protection Officer)
- why the personal data is needed, and how it will be used
- whether the personal information will be shared, and with whom
- how long the data will be kept
- whether the data will be used for profiling or to make any automated decisions (i.e. decisions that are made without human intervention)
- how to make a complaint

If the personal data is collected from a child, the privacy notice must be in language that they will understand.

All forms (paper and electronic) must be redesigned to reflect these new requirements.

Sharing Information

The Council often shares information with partners, like the NHS, Housing Associations, or the Voluntary Sector, in order to provide services. We must ensure we follow the data protection principles whenever personal data is shared. It's important to make sure that:

- the data subject has an awareness about who might receive their personal data (the exception to this is if the information is required to investigate crime)
- there is a valid condition for processing
- only necessary and relevant personal data is shared
- a record is kept of what personal data is shared and why

If personal data is shared routinely with another organisation, the arrangement must be underpinned by an appropriate information sharing agreement. The manner of sharing will also need to be documented within a Data Protection Impact Assessment (DPIA).

GDPR

Managing Breaches

If an organisation collects and uses personal data, but fails to follow the data protection principles, it commits a data protection breach. A breach will happen if personal data is lost, stolen, or not adequately protected so it can be accessed by someone who should not see it.

Breaches can be caused by mistakes, by not following Council procedure, or by not having appropriate procedures or controls in place. All colleagues must complete Data Protection and Data Security training on Clacks Academy to help prevent mistakes from happening and to evidence that, when they do occur, breaches are a result of a genuine error rather than ignorance.

All potential data protection breaches must be reported to the Data Protection Officer immediately so they can be assessed, reported and investigated appropriately.

Under the new Data Protection Act, it will be mandatory to report some serious breaches to the ICO within 72 hours of identification. Failure could result in the Council being fined.

Fines

These are substantial – up to £17million or 4% of global turnover.

GDPR

Individual Rights

Under the new Data Protection Act, individuals have a right, to:

- be informed about what will happen to their personal data. This will be managed through privacy notices
- access personal data held about them. This right exists under current legislation (subject access requests) however organisations will have a shorter period to provide information (30 days)
- have inaccurate personal data amended
- object to certain types of processing
- restrict automated decision-making and profiling
- have their personal data deleted. This 'right to be forgotten' will only apply in certain circumstances
- have their personal data transferred directly to another data controller. Again will also only apply in certain circumstances

Data Processors

The Council uses third party suppliers to help us deliver services, for example, when we use care providers. When we use systems that are provided by third party suppliers, or outsource work to other organisations, the other organisation will be classed as a Data Processor under data protection legislation.

Data processors will have access to, and use personal data collected by the Council so it's important that their data protection responsibilities are included within contract arrangements. The need for appropriate contract clauses can be identified and recorded through the Data Protection Impact Assessment (DPIA) process so it's important that these are completed when new systems are purchased or new ways of working adopted.

Under the Data Protection Act 1998, data processors were not liable for data protection breaches processed on behalf of another data controller, however, under the new legislation they will be.

GDPR

General Data Protection Regulation

Clackmannanshire Council | Comhairle Siorrachd Chlach Mhanann
www.clacks.gov.uk