Inverclyde Council

General Data Protection Regulation 2018

General Data Protection Regulation (GDPR)

Employees' guide

Inverclyde council

Introduction

Data protection law is changing on 25 May 2018.

This guide will help you understand what is changing and what this means for you as an employee who may handle personal data as part of your role.

Activity is already taking place to get the Council ready for this change and it is important that you read this guide to know what is happening.

This guide will be supported by a mandatory e-learning course for all staff who have access to a computer and deal with personal data.

What is Data Protection?

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 current Data Protection Act 1998 regulates the way personal data is handled and processed. It gives individuals certain rights and protects them from the potential misuse of their personal data. However, this law was brought into force before the Internet explosion and so, it does not reflect many of the practices now deemed common place amongst global businesses.

The existing law will be replaced by the General Data Protection Regulation (GDPR). The GDPR is an EU Regulation. It will become law automatically when it comes into force on 25 May 2018. A Data Protection Bill is also making its way through Parliament. The Bill will fill in the gaps in the GDPR where Member States have been allowed to make their own rules.

You may have heard talk about the GDPR already within your Service. The GDPR will enhance existing rules and introduce some new rules on how the Council collects and processes personal data. It has been created to strengthen the rights of individuals and protect personal data in the digital age.

The GDPR and Data Protection Bill are referred to collectively as the new Data Protection Laws throughout this guide.

You need to be aware of what these changes mean for you if you handle or process personal data as part of your role.

The General Data Protection Regulation - what's changing?

The new Data Protection Laws give individuals, for example, our customers and service users, more power and control over how their personal data is handled by organisations such as the Council.

The main changes the Council requires to implement are to:

- be much more open with our customers about what we do with their data;
- introduce new documenting procedures;
- perform data privacy impact assessments;
- make sure we only collect and use the minimum amount of personal data needed to get the job done;
- rely on "consent" as the legal basis for processing as a last resort;
- strengthen our rules for deleting and removing personal data;
- notify the ICO and potentially our customers if a personal data breach occurs.

You will find more detail on each of these changes within this guide.

In the UK, the UK Information Commissioner (www.ico.org.uk) will continue to be the regulator ("ICO"). The ICO will continue to provide advice and guidance about data protection to organisations and individuals. The ICO will also continue to investigate complaints, assess breaches and take enforcement action where required. This will include criminal prosecution in certain circumstances.

What are the Data Protection Principles?

The new Data Protection Laws provide a governance framework based on six principles which 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. The Council must tell individuals very clearly what they intend to do with the personal data collected about them.

Purpose Limitation

Personal data should be collected for specific, explicit and legitimate purposes. If the Council has collected personal data, and told the individual what the Council 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. The Council 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 the Council holds 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. The Council's systems and processes should be designed to delete personal data as soon as it is no longer needed and in accordance with the Council's Policy for the Retention and Disposal of Records. 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.

NOTE	Data protection principles apply to personal data captured in all formats, including hardcopy paper, electronic systems and CCTV.

HANDY HINT	If you're unsure about whether processing meets these six principles, conduct a Data Protection Impact Assessment or contact the Information Governance Team at dataprotection@inverclyde.gov.uk to seek advice

What is personal data and when can I use it?

Personal data is information which relates to a living individual ("Data Subject") who can be identified from the information itself or by linking it with other information.

For example:

- a person's name and address;
- an online profile;
- a member of staff's HR record; or
- records relating to an individual such as school pupils or service users.

Certain types of personal data need added protection and can only be processed if certain conditions apply. This data is known as Special Category Data. Special Category Data is personal data which reveals or comprises:

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

NOTE	Processing relates to any use of personal data including, collecting, using, sharing, storing and deleting
HANDY HINT	If you're unsure whether personal data falls within a Special Category contact the Information Governance Team at dataprotection@inverclyde.gov.uk.

When can I process personal data?

Processing is the name given to anything that the Council does with the personal data that we hold – for example entering customer information into our IT systems or simply having a competed form sitting in a filing cabinet.

We can process personal data if at least one of the following conditions is satisfied:

- for the **performance of a contract**. For example if it's in accordance with an employment contract, or as part of a contracted service;

- to enable the Council to comply with a **legal obligation** for example 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 however, 'vital interest' has a high benchmark and will normally relate to potential life or death scenarios;

- for the performance of **a task which is carried out by the Council in the public interest** or in its official authority ("public task"). This is likely to cover processing required to deliver Council services like Social Work and Education;

- where the individual has given **Consent.** The new Data Protection Laws make processing personal data based on consent more restrictive, in particular, consent must be freely given. However, as the balance of power between the Council and individuals is not an equal playing field, establishing freely given consent is likely to be difficult for the Council. The Council should therefore rely on consent as a last resort and where it is relied upon, a record should be made explaining how the consent was freely given;

- where the processing is necessary for the **Legitimate Interests** of the Council or a third party, except where such interests are overridden by the interests, rights or freedoms of the Data Subject. The legitimate interests will need to be set out. The Council can only consider relying on this condition where there is no "public task" covering the situation concerned.

The six conditions detailed above are known as 'conditions for processing'.

When can I process Special Category Data?

The processing of Special Category Data is prohibited unless at least one of the following additional conditions for processing is satisfied:

- 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;

  to protect someone's vital interest, for example, to respond to child protection concerns - remember 'vital interest' normally has to relate to potential life or death scenarios;

- to establish, exercise or defend legal claims;

And

- for reasons of substantial public interest based in law;

- for preventative or 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, for example, to provide occupational health services, or deliver health and social care services;

- for reasons of public interest in the area of public health;

- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with the law;

  Or

- if the personal data has been made public by the Data Subject;

- if the Data Subject has given explicit consent.

HANDY HINT	If you're unsure about what conditions might apply, contact the Information Governance team at dataprotection@inverclyde.gov.uk for advice.

What Changes will the new Data Protection Laws introduce for the Council?

This section gives an overview of the main changes introduced by the new Data Protection Laws and what these changes will mean for the Council. (Appendix 1 shows a comparison table).

Data Protection Officer

Public Bodies, such as the Council, are required to appoint a Data Protection Officer ("DPO"). This is an officer with responsibility for advising the Council on its Data Protection obligations, including the risks associated with carrying out certain actions and processes. The DPO also monitors the Council's internal compliance with the new Data Protection Laws. They act as a 'critical friend' and will advise the Council's Corporate Management Team about whether the Council is meeting its responsibilities under GDPR.

The Council's DPO is Andrew Greer. He is contactable at dataprotection@inverclyde.gov.uk

Consent

The new Data Protection Laws aim to ensure that consent is specific to the particular purpose of processing. Silence or inactivity does not constitute consent. Consent can be evidenced where an individual has been fully informed, through privacy information, of how their data will be processed and has freely given their consent to that processing. Consent is not freely given if the individual really has no choice in the matter, for example, where the Council must provide the service.

Where the Council delivers its statutory functions, consent will not be a lawful condition for processing. In such circumstances, it is likely to be more appropriate to rely on "public task" or "compliance with a legal obligation" as the lawful condition for processing.

Consent should only be used as a last resort and when it can be freely given. A record should be kept including what was said to the customer about how their personal data would be used, who gave the consent and when this was given. The customer must also be informed that they should contact the Council's Data Protection Officer mentioned below should they wish to withdraw consent.

Individuals' Rights

Under the new Data Protection Laws, individuals have the following rights:

- to be informed about what will happen to their personal data. The Council will need to give more information to its customers. This will be managed through privacy notices as explained in further detail in the next section;

- to access personal data held about them. This right already exists under the current Subject Access Request ("SAR") process. However, the response will have to be provided within 30 days. That said, in certain cases, where there is a lot of material, this may be extended by 2 months. SARs must also be provided free of charge. However, a "reasonable fee" can be charged where the request is manifestly unfounded or excessive. The Council's existing SAR processes will be updated;

- to have inaccurate personal data amended;

- to object to certain types of processing;

- to have their personal data deleted. This 'right to be forgotten' will only apply in certain circumstances;

- to restrict automated decision-making and profiling; and

- to have their personal data transferred directly from the Council to another Data Controller. Again this will also only apply in certain circumstances.

If a Data Subject wishes to exercise any of their rights under the new Data Protection Laws, their request must be passed to the Information Governance Team immediately.

HANDY HINT	www.inverclyde.gov.uk/home/FAQ's/Dataprotection/How can I see what personal data of mine that the Council holds?

Accountability

There is a greater focus on accountability which means, in addition to complying with data protection principles, organisations will have to be able to demonstrate that they comply, particularly through the documents and records they keep. Being accountable includes understanding what personal data the Council holds. The Council will gain this understanding by having an Information Asset Register.

Records also require to be kept throughout the Council by Services, for example, when personal data is shared and where a Data Privacy Impact Assessment is undertaken. Data protection breaches must be recorded.

Part of the Accountability principle is also to have appropriate data protection policies and procedures in place. You should already be aware of and be following existing policies such as the Council's Acceptable Use of Information Systems Policy, Information Classification and Guidance and the Clear Desk Policy, to promote good information handling practice.

Data Protection Impact Assessments

Data Protection Impact Assessments (DPIAs) will become mandatory for processing activities where, for example, there is likely to be a high risk to the rights and freedoms of individuals. Where the processing is particularly high risk, it may be necessary to seek the authorisation of the ICO.

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.

Where risks are identified, it will be necessary to put controls in place to reduce or remove such risks. Examples of controls include identifying and collecting only the minimum amount of personal data required for the processing, managing who has access to the personal data, providing appropriate security, ensuring that Data Subjects know how the Council is using their data through privacy information and deleting the personal data or using annonymisation techniques when the data is no longer required.

DPIAs provide evidence that the Council has considered data protection principles when designing processes that handle personal data. They document and evidence that the Council has tried to do the right thing.

Further guidance on Data Protection Impact Assessments will be made available.

Privacy by Design

Privacy by Design involves implementing measures which show the Council has considered and embedded data protection into its processing activities. Privacy by Design promotes the protection of personal data from the start, for example, when building a new IT system which will process personal data. Data Protection Impact Assessments (DPIAs) are an integral part of Privacy by Design. Annonymising personal data and collecting only the minimum amount of personal data required for the processing activity are also examples of Privacy by Design.

A new Privacy by Design framework will be introduced.

Sharing Information

The Council often shares information with partners, like the NHS, Housing Associations, or the Voluntary Sector, in order to provide services. The Council 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 (there are exceptions to this including if the information is required to investigate crime);
- there is a valid condition for processing;

- only necessary and relevant personal data is shared; and
- 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 Data Sharing Agreement (DSA) based on the Council's Information Sharing Protocol. The manner of sharing may also need to be documented within a Data Protection Impact Assessment.

All DSAs must be submitted to the Information Governance Team for review before they are signed. All signed DSAs will be logged. Unless you advise otherwise due, for example, to confidentiality, DSAs will be available on ICON so that officers can see what DSAs the Council has in place.

The Council's Information Sharing Protocol and style DSA will be updated. Existing DSAs will also require to be reviewed to ensure they comply with the new Data Protection Laws.

Data Processors

The Council uses third party suppliers to help deliver services, for example, care providers. When the Council outsources such work to other organisations or uses systems that are provided by third party suppliers, the other organisation will be classed as a Data Processor under data protection legislation. Data Processors have access to and use personal data collected by the Council.

Under the Data Protection Act 1998, Data Processors were not liable for data protection breaches, the Data Controller - i.e. the Council - remained responsible. However, under the new Data Protection Laws fines can be imposed directly on Data Processors for certain breaches.

The Council must still ensure that any Data Processor it appoints demonstrates that it complies with the new Data Protection Laws. So, it is important to include data protection responsibilities within the tender process and the contract. The need for appropriate contract clauses can be identified and recorded through the Data Protection Impact Assessment process. It's important that such assessments are completed when new systems are purchased or new ways of working adopted.

The Council's standard terms and conditions are currently being updated to include appropriate GDPR clauses and consideration is being given to how to include appropriate data protection checks within tender processes.

Breach notification

All data protection breaches must be reported to the ICO other than minor breaches. Organisations will have only 72 hours after a breach of personal data has been discovered to notify the ICO. Data Subjects may also have to be notified if the breach is high risk.

A breach will occur if, for example, 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 officers must complete Information Governance training 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.

It is critical that you report any breach in data protection to your line manager immediately.

If you suspect a breach might have occurred follow the Council's Data Breach Management Protocol on ICON.

Fines

The GDPR introduces substantially higher fines where a breach is found to have occurred. For the Council this could mean a fine of up to £8million. So it is important to get it right first time when dealing with customers' data.

HANDY HINT	If you're unsure about whether something is a data protection breach or if it is a minor breach always contact the Information Governance Team to seek advice

HANDY HINT	The Information Governance Module is available on Brightwave e-learning under mandatory/induction.

How will the new Data Protection Laws change how the Council interacts with customers?

Transparency and openness – privacy statements

The current data protection rules require the Council to give customers certain information about who the Council is and what the Council will do with their data, or at least to make this information available to them. Normally this is done by means of a short privacy statement at the bottom of forms, which should ideally refer the customer to our web site where a more detailed description is available under the Council privacy statement.

Under the new Data Protection Laws, this requirement is significantly enhanced and the Council will need to communicate more clearly to customers on how the Council will use their information. The information which the Council will require to provide includes:

- details of what personal data the Council processes;
- the legal basis for the processing;
- how long the Council will keep the information;
- who the Council share the information with;
- the rights customer have, for example to restrict processing and to complain to the ICO; and
- a contact point for any queries regarding the processing activities - being the Data Protection Officer mentioned above.

The Information Governance Team is currently developing a new Privacy Information Notice for the Council's Website. In addition to this, all forms used by Services will also need to be re-designed to reflect the new requirements.

Consent as a lawful basis for processing

As previously explained, where the Council is delivering a statutory function, consent will not be the appropriate lawful condition for processing because the consent will not be seen to be feely given. In such circumstances, it is likely to be more appropriate to rely on the "public task" or "compliance with a legal obligation" as the lawful condition for processing. However, if the Council is going beyond core statutory functions, it may still be appropriate to rely on consent provided the new and more stringent rules explained in the last section are followed.

Why it is beneficial for the Council to comply with the new Data Protection Laws?

Develop stronger processes

The new Data Protection Laws will help the Council to enhance existing good information governance in relation to the personal data that the Council handles and demonstrate to the Council's customers that we value their privacy.

More efficient

The new Data Protection Laws will help the Council to streamline processes and reduce duplication that may exist.

Privacy by Design

Elements such as Privacy by Design will help the Council to make sure that operational processes are planned to:

- respect the rights and privacy of our customers;
- keep their personal data safe;
- avoid disruption;
- avoid damage to our reputation; and
- drive the quality of the services we provide.

Better use of technology

The new Data Protection Laws will allow the Council to make the best use of our technology to support the personal data, for example, to support the way we store as well as the way we share personal data.

Fines

As previously explained, the Council could be fined up to £8million for a serious data protection breach – a sum which would have a major impact on key services and the resources required to deliver them.

Where can I learn more?

There is information about the new Data Protection Laws and other areas of information governance on ICON. Search for the Information Governance pages to find out more about Data Protection Impact Assessments (DPIAs), Privacy Notices, Information Sharing, Records Management, and Individual's Rights. There is also an Information Governance e-learning module. Look under Council Information and Policies on ICON and click Brightwave E-learning and select Information Governance.

A new GDPR e-learning module will also be made available.

Advice and assistance - who can I ask for help?

The Council's Information Governance Team can provide advice on all areas of data protection and information governance compliance. Contact the team at dataprotection@inverclyde.gov.uk

GDPR Compliance Checklist

Do these things to keep yourself right:

- ✓ **Complete the Information Governance e-learning module.**
- ✓ **Look under Council Information and Policies on ICON and click Brightwave E-learning and select Information Governance;**
- ✓ **undertake the mandatory GDPR e-learning module when this becomes available;**
- ✓ **ensure you are familiar with the new Individuals' rights;**
- ✓ **ensure there are documented procedures to guide colleagues on how to handle personal data;**
- ✓ **identify information risks in your area and manage them through Service Risk Registers;**
- ✓ **Understand the Council controls in place, and when to use them:**
  - o **Data Protection Impact Assessments;**
  - o **Privacy Notices;**
  - o **Data Protection Breach Management process;**
  - o **Acceptable Use of Information Systems;**
  - o **Information Classification;**
  - o **Information Sharing arrangements;**
- ✓ **Follow the Council's retention rules:**
- ✓ **Policy for the Retention and Disposal of Documents and Records Paper and Electronic;**
- ✓ **Be familiar with the Council's Record Management Manual;**
- ✓ **Identify service user and customer forms used by your Service and determine whether they are GDPR compliant;**

- ✓ **Ensure existing supplier contracts and Information Sharing Agreements which involve the processing of personal data are GDPR compliant; and**
- ✓ **Contact the Information Governance Team if you have any questions on data protection and information governance compliance at dataprotection@inverclyde.gov.uk**

Data Protection – it's changing

Appendix 1 Key Data Protection Changes from May 2018

TOPIC	EXAMPLE	EXISTING DATA PROTECTION ACT 1988	FROM 25 MAY 2018 NEW GENERAL DATA PROTECTION REGULATION (GDPR)
Breach of data protection	This is where the Council have to notify our data protection regulator – the Information commissioner – if we have lost any personal data. For example: A paper notebook containing personal details of customers was lost and handed to a local newspaper. The notebook was recovered but not before the newspaper published a story about the incident.	• Currently it is only best practice to report high risk breaches to the regulator • Council policy is to formally assess breaches and report to the regulator in line with the best practice • The Council are not obliged to inform individuals affected by the breach	• The Council will have 72 hours to report breaches to the regulator • All breaches must be reported unless there is a minimal risk to the rights and freedoms of those affected • The Council must inform individuals who are affected where there is a high risk to those individuals

Being fined for a data protection breach	The Council can receive a fine for breaching Data Protection Laws – such as losing personal data. For example: in 2013 a local authority lost an encrypted laptop containing the personal details of over 20,000 individuals and they were fined £150,000	• Currently the Council can be fined up to £500,000	• Greater penalties are in place – up to 4% of global annual turnover of the preceding year – whichever is greater. For example: For the Council 4% of global annual worldwide turnover means the Council could be fined up to £8 million
Data Protection Officer	This is a dedicated senior Council officer who has a role to enforce how the Council collect and process personal data in line with Data Protection Laws	• Currently not a mandatory role	• As a public authority this is a mandatory role and the Council have appointed a Data Protection Officer
A subject access request	This is where an individual can contact the Council to see what information we hold about them. For example: A citizen could ask to see all the information that Finance holds on them.	• Currently the Council have 40 calendar days to respond • The Council can charge £10 fee • The Council do not incur any fines for a late response	• The Council must respond without due delay and at the latest within one month • The Council cannot charge a fee • For consecutively late responses we could be • fined up to £17 million or 4% of global annual turnover of the preceding year whichever is greater. • For example: for the Council 4% of global annual worldwide turnover means we could be fined up to £8 million
Privacy notices	A key principle of the new Data Protection Laws is that all personal data should be processed fairly and lawfully. Fair	• Privacy notices are required to allow individuals to understand what their personal	• Individuals will need a lot more information to be supplied to them under the new regulation – so that

	processing includes telling individuals that the Council hold their information and what we will do with it. For example: Where we have a notice or a form on our website that explains how personal data is processed.	information is being used for	they can better understand what information the Council hold on them and why. • Privacy notices will need to be easily accessible, clearly communicated and easily understood

Legal and Property Services
Municipal Building
Clyde Square
Greenock
Inverclyde PA15 1LY