# PEMBROKESHIRE COUNTY COUNCIL

## GUIDANCE NEWSLETTER

## *GENERAL DATA PROTECTION REGULATION (GDPR)*


## AUDIT, RISK & INFORMATION SERVICE

## DATE TO REMEMBER:

## "25 MAY 2018"

The EU General Data Protection Regulation (GDPR) will come into effect from this date.

If you handle personal data in your role, it is essential that you are aware of the requirements.


Data Protection requirements have been in place for many years, and although the GDPR broadens the requirements particularly in relation to demonstrating accountability and transparency, many of the key principles are similar to those in the Data Protection Act 1998.

We all handle personal data as some point within the working environment so it important that we understand our legal obligations.

This guide explains the purpose and effect of each principle, gives practical examples and highlights common errors that result in breaches.

This guidance newsletter will provide you with useful definitions that you must have an understanding of in relation to the GDPR.

Pembrokeshire County Council is committed to ensuring the highest standards of Data Protection. We will treat all personal data as we would expect our own personal data to be treated, i.e. with respect, integrity, confidentiality and in accordance with the GDPR and other Data Protection laws. In order to demonstrate our commitment to the highest standards of Data Protection, the Chief Executive and the Leader of the Council will be signing up to the Information Commissioners 'Personal Information Promise' in May 2018.


Further information on the 'Personal Information Promise' can be found on the ICO website.

## USEFUL DEFINITIONS

Here are some key words referred to as part of the GDPR and used throughout this guidance newsletter:

- **Data Subjects**
  Means an individual who is the subject of personal data.

- **Personal Data**
  The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular to an identifier, e.g. name, identification number, location data, or online identifier.

- **Special Category Data (Sensitive Personal Data)**
  Special category data is personal data which the GDPR says is more sensitive:
  - Race
  - Ethnic origin
  - Politics
  - Religion
  - Trade union membership
  - Genetics
  - Biometrics (where used for ID purposes)
  - Sex life or sexual orientation

- **Data Controller**:
  This is the body which determines the purposes for which personal/special category data is processed. The Council as a whole is classed as a Data Controller, which covers the vast majority of our personal data processing. Individual schools are classed as Data Controllers.

- **Data Processor:**
  In some circumstances we may commission another body to undertake processing activities on our behalf, e.g. confidential waste disposal, postal service.

## THE SIX GDPR PRINCPLES

As a Data Controller, we are accountable and must be able to evidence our compliance with the following GDPR principles. Such evidence would include training records, fair processing notices and maintaining an up to date Information Asset Register.

1. **Lawfulness, Fairness and Transparency**
   Personal data can only be processed if there is a lawful reason for doing so. You must have legitimate grounds for collecting and using personal data. You must be transparent about how you intend to use the data and give individuals appropriate privacy notices when collecting their personal data.

2. **Purpose Limitation**
   The data must be collected for specified, explicit and legitimate purposes and shall not be further processed in any manner incompatible with that purpose. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is permitted in certain circumstances.

3. **Data Minimisation**
   Personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

4. **Accuracy**
   Personal data shall be accurate and where necessary kept up to date. Reasonable steps should be taken to ensure the accuracy of any personal data you obtain and ensure the source of any personal data is clear.

5. **Storage Limitation**
   Personal data must be kept in a form which permits identification of data subjects for no longer than necessary, for the purposes for which the personal data is processed. Personal data may be stored for longer periods solely for archiving purposes.

6. **Integrity and Confidentiality**
   Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction and damage, by using appropriate technical or organisational measures.

## PROCESSING PERSONAL DATA

***Q: Do you know the Legal Basis for processing personal data within your role?***

***A: Processing of personal data is only lawful if one of the following apply:***

1. **Consent**
   The data subject has given clear consent for you to process their personal data for one or more specific purpose. This can be withdrawn at any point.

2. **Contract**
   Processing personal data is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. (E.g. Gym Memberships, Tendered Contracts (Procurement), Contract of Employment (HR) etc.

3. **Legal Obligation**
   Processing personal data is necessary for compliance with a legal obligation to which the Data Controller is subject.

4. **Vital Interests**
   Processing personal data is necessary in order to protect the vital interests of the data subject or another person. E.g. Safeguarding, Next of Kin Contact Details (HR).

5. **Public Task**
   Processing personal data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority. E.g. Social Services, Education.

6. **Legitimate Interests**
   Processing personal data is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

## PROCESSING SPECIAL CATEGORY DATA

Under GDPR this data is classed as more sensitive and needs additional protection. In order to process special category data, you must have a legal basis and satisfy a separate condition for processing. There are 10 conditions for processing under GDPR, but the UK Data Protection Bill will introduce further conditions and safeguards.

## INDIVIDUAL'S RIGHTS

GDPR extends the rights of individual's (data subjects) in order to access and protect their personal data. Some of these rights existed under the Data Protection Act but have been strengthened under GDPR.


**How do we observe the rights of individuals within Pembrokeshire County Council to ensure compliance?**

## RIGHT TO BE INFORMED

Under GDPR there is a requirement for the Council to be transparent about the information we hold, how we use it, how long we intend to keep it for and who we share it with. This is known as privacy information. We must provide this information to individuals at the time we collect their data.

If we obtain personal data from other sources, we must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month. There are a few circumstances when you do not need to provide people with privacy information, such as if an individual already has the information or if it would involve disproportionate effort.

Our privacy notices must be concise, transparent, intelligible, easily accessible, and we must use clear and plain language. If we intend to use an individual's data for a new purpose, we must bring it to their attention before we start processing it for the new purpose.

We have created a Privacy Notice template which will be available on the Audit, Risk & Information Service intranet page.

**If we get this right, we will gain our customers confidence and trust! If we get it wrong then we could face reputational damage and fines!**

## RIGHT OF ACCESS

Customers of Pembrokeshire County Council have the right to access their data via a 'Subject Access Request'. Requests must be processed within one calendar month.

The Access to Records Analysts coordinate all requests for personal data. They have the knowledge, experience and software to ensure that information released to data subjects is redacted to protect any third party personal data.

Any Subject Access Requests received by staff members must be sent to the Access to Records Analysts for processing without delay using the following contact details: accesstorecords@pembrokeshire.gov.uk

From 25 May 2018 we must provide this information free of charge. The timescale for providing this information has been reduced from 40 working days to one calendar month, therefore we need your cooperation to ensure that requests are promptly passed to the team for processing.

## RIGHT TO RECTIFICATION

We must ensure that data we hold on an individual is complete, accurate and kept up to date. Staff must ensure reasonable steps are taken when data is reported as being inaccurate or incomplete to ensure it is corrected without delay. We have one calendar month to respond to a request which can be received verbally or in writing.

There are certain circumstances where a request can be refused, your Line Manager or the Information Governance Team will be able to advise further.

**Failing to update systems and records when notified of changes of address, or other personal data is a common cause of a data protection breach. Primary records must be maintained as they will be the source for decision making and communicating.**

## RIGHT TO ERASURE

Under certain conditions, customers can make a request for their personal data to be erased. This is also known as the *"right to be forgotten".* Some examples of when this would apply include:

- The personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
- Where the legal basis for processing is consent, the data subject withdraws his or her consent for us to use it
- The personal data has been processed unlawfully
- If personal data is being processed for the purposes of direct marketing and the individual objects to it.


The *"right to be forgotten"* only applies where the above conditions are met and there are further exemptions where we can refuse to comply with a request:

- If it conflicts with the "right of freedom and expression"
- An overriding need to adhere to legal compliance
- Reasons for public interest in the area of public health
- Scientific, historical research or public interest archiving purposes
- If the data is required for supporting legal claims.

Alternatively, please contact the Information Governance Team:
dataprotection@pembrokeshire.gov.uk

## RESTRICT PROCESSING

Individuals have the right to request the restriction or suppression of the processing of their personal data, where one of the following conditions apply:

- Accuracy has been challenged
- Processing is unlawful
- The Council no longer needs the personal data for the purposes of the processing, but the individual needs us to keep it in order to establish, exercise or defend a legal claim
- The individual has objected to the Council processing their personal data under the legal basis of public task or legitimate interests, and the Council is considering whether our legitimate grounds override those of the individual.

Requests are legitimate whether they are received verbally or in writing and we have one calendar month to comply with the request.

How we restrict processing will depend on the type of processing. If you receive a request you should refer it to your Line Manager.

## DATA PORTABILITY

The Right to Data Portability is unlikely to apply to any services provided by the Council. This right allows individuals to obtain and reuse their personal data for their own purposes across different services. This right will be more applicable to utility services, mobile phone providers, banks, etc.

## OBJECTING TO DATA USE

Individuals have the right to object to:

- Processing where the legal basis used is 'legitimate interests' or 'the performance of a task in the public interest/exercise of official authority (including profiling)'
- Direct marketing (including profiling)
- Processing for purposes of scientific/historical research and statistics.

To demonstrate compliance with the GDPR first principle, 'Lawfully, Fairly and Transparency' you must maintain a record of any request made under the right to object to processing and notify the Information Governance Team of your actions.

Review existing processes to ensure that marketing communications are kept up to date, including an option to positively opt-in to receiving marketing communications.

**ICO Enforcement**

The Royal Mail Group Limited were fined £12k for sending out over 300,000 nuisance emails to people who had already opted out of receiving direct marketing.

## OTHER COMPLIANCE REQUIREMENTS

### INFORMATION ASSET REGISTER (IAR)

One of the GDPR requirements is to maintain a record of all the processing activities that take place within the Council. We need to identify:

- what personal data we process;
- what is the lawful basis for processing;
- how we store and keep the data secure;
- who has access to it;
- who we share the data with and what sharing agreements are in place;
- how long we keep it for.

The Council's Information Asset Register is held on the MKInsight system and identifies all the services/systems that hold personal data.

The Information Asset Register will provide an overview for all data processing activities within the Council, and will therefore enable us to demonstrate to the Information Commissioner what personal data is being processed, by whom and why.

The Information Governance Team will have met with a responsible officer from your service area to determine the information to include within the IAR. Compliance checks have been undertaken to identify areas for improvement and to provide an accurate risk assessment of processing activities across the Council.

### DATA SECURITY

Failing to follow security procedures is what results in the majority of data breaches. There are numerous IT policies, procedures and forms which are available on the Intranet and these define data security expectations which will assist you to comply with the GDPR. You have a responsibility to read, understand and adhere to these policies and procedures.  Failure to adhere to these policies and procedures could result in disciplinary action. If you are unsure of data security requirements please seek clarification from your Line Manager or the Information Governance Team.

**ICO Enforcement Action**

ICO fined the Royal Borough of Kensington & Chelsea £120k for an error that resulted in the unlawful identification of 943 people who owned vacant properties in the area. This was a result of copying hidden information from one spreadsheet to another without realising and releasing under an FOI request.

**ICO Enforcement Action**

A former employee of Southwark Council has been prosecuted for illegally obtaining and sharing information about school children and their parents.

## STORING DATA

Customers have the right to ensure that their data is not kept by us any longer than necessary. The Council follows a Retention Guideline for Local Authorities that identifies how long data should be kept for.

Staff must ensure we do not hold data any longer than required. All data we hold is open to Subject Access Request (SAR's) and Freedom of Information Requests (FOI's). If you are unsure of data retention periods within your service area please contact Sarah Bevan in Records Management: sarahbevan@pembrokeshire.gov.uk

Loss of data must be reported immediately to the Data Protection Officer so the breach can be investigated: dataprotection@pembrokeshire.gov.uk

**ICO Enforcement Action**

Humberside Police were fined £130k after disks containing a video interview of an alleged rape victim went missing. The unencrypted disks were left on an officer's desk and were intended to be sent to another Police force by unsecure mail. There was no audit trail of what happened to the package.

**ICO Enforcement Action**

Norfolk County Council were fined £60k for leaving files that included sensitive information about a child in a cabinet that was sent to a second hand shop.

Hampshire County Council were fined £100k after documents containing personal details of over 100 people were found in a disused building.

## DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

The GDPR introduces a new obligation to do a DPIA before carrying out processing likely to result in high risk to individuals' interests. If your DPIA identifies a high risk which you cannot mitigate, you must consult the ICO. The Data Protection Officer must review and sign-off all DPIA's.

This is a key element of the new focus on accountability and data protection by design, and a more risk-based approach to compliance.

In particular, the GDPR says you must do a DPIA if you plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

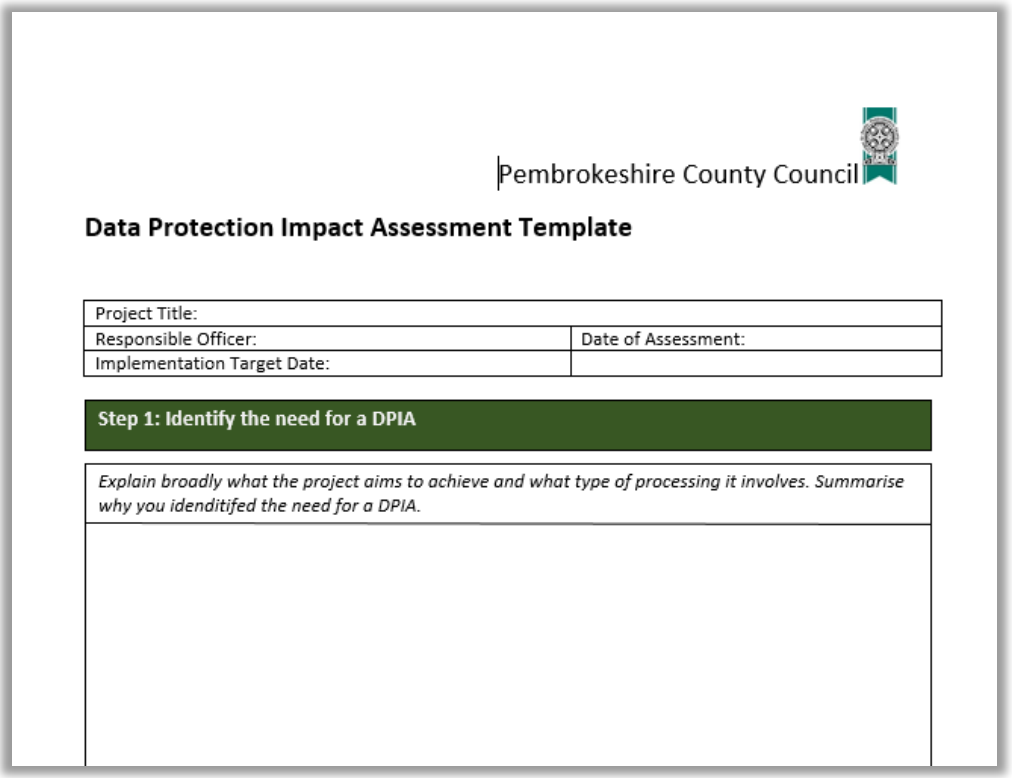
The ICO also requires the Council to do a DPIA if we plan to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behavior;
- profile children or target services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

You should also think carefully about doing a DPIA for any other processing which is large scale, involves profiling or monitoring, decides on access to services, or involves sensitive data or vulnerable individuals.

Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data.

A link to our DPIA template is available on our Audit, Risk & Information Service intranet page.



Pembrokeshire County Council

**Data Protection Impact Assessment Template**

| | |
|---|---|
| Project Title: | |
| Responsible Officer: | Date of Assessment: |
| Implementation Target Date: | |

**Step 1: Identify the need for a DPIA**

| |
|---|
| *Explain broadly what the project aims to achieve and what type of processing it involves. Summarise why you idenditifed the need for a DPIA.* |
| |


The focus is on the 'residual risk' after any mitigating measures have been taken. If your DPIA identified a high risk, but you have taken measures to reduce this risk so that it is no longer a high risk, you do not need to consult the ICO.

## REPORTING DATA BREACHES


A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A data incident, is a breach of security that could have, but did not lead to one of the above.

Any data incidents or breaches must be reported immediately to the Data Protection Officer via the Information Governance Team. The Data Protection Officer is responsible for reporting data breaches to the Information Commissioners Office and undertaking an investigation.

Under GDPR we will have to notify the Information Commissioners Office of serious breaches within 72 hours of discovery of the breach. Failure to report a breach within the timeframe could itself result in a fine, as well as a fine for the breach itself.

An e-form will be available on the Intranet "Notification of Data Breach" to report a data breach or you can email dataprotection@pembrokeshire.gov.uk.

## Key Actions!


1. If there is a high risk to the data subject from the breach, they need to be informed straight away so they can take actions to protect themselves. Seek advice from the Data Protection Officer!
2. Containment is key! If we can retrieve the data from an unauthorised recipient, do so straightaway;
3. When retrieving the data from them, confirm that no copies of the data have been made or shared;
4. Ask if they have read the whole document or just parts and if they know the person who should have initially received this information.
5. Report the breach: dataprotection@pembrokeshire.gov.uk

## DATA PROTECTION OFFICER (DPO)

There is a statutory requirement for the Council to appoint a Data Protection Officer under GDPR. The Data Protection Officer is responsible for assisting the Council to monitor compliance, informing and advising on data protection obligations, providing advice on Data Protection Impact Assessments and acting as a point of contact for data subjects and the Information Commissioners Office.

### Contact Details of DPO:

**Jo Hendy**,
Governance, Assurance & Information Manager, ext. 6213
joanne.hendy@pembrokeshire.gov.uk

The tasks of the DPO include:

- Informing and advising anyone acting on behalf of the Council of their data protection obligations,
- Monitoring compliance with Data Protection Laws, which includes monitoring compliance with the Council's policies and procedures, managing internal data protection activities, raising awareness of data protection issues and training staff, Members, Volunteers, etc.
- Ensuring the Information Asset Register (IAR) is an active register that identifies all systems that hold personal data;
- Advising on the necessity of data protection impact assessments (DPIA), the manner of their implementation and outcomes;
- Serve as the contact point for all data protection issues, including managing risks and data breach reporting;
- Serve as the contact point for individuals (data subjects) on privacy matters, including Subject Access Requests.

### Further Contact Details:

**Contact for Data Protection:**
Information Governance Team, ext. 5644
DataProtection@pembrokeshire.gov.uk

**Contact for Subject Access Requests**
Access to Records Analysts, ext. 5798
accesstorecords@pembrokeshire.gov.uk