Older People's Commissioner for Wales
Comisiynydd Pobl Hŷn Cymru

PRIVACY AND DATA PROTECTION POLICY

Version	5.0
Review Date	September 2020
Reviewed	March 2018
Responsible Manager	Director of Corporate Affairs

Older People's Commissioner for Wales
Comisiynydd Pobl Hŷn Cymru

Privacy and Data Protection Policy

Purpose

This policy sets out the Older People's Commissioner for Wales' obligations in relation to personal information under the Data Protection legislation (which includes the General Data Protection Regulation ("**GDPR**")). It also sets out the Commissioner's approach to personal information and the requirements on staff to ensure the proper handling of all personal information within the organisation.

The Act gives individuals the right to know what information is held about them. It also provides a framework to ensure that personal information is handled properly.

Personal Information

Personal information means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way we collect information about people.

The Data Protection legislation applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the Data Protection legislation depending on how difficult it is to attribute the pseudonym to a particular individual.

The Principles

The Data Protection legislation states that anyone who handles person information must comply with six principles, which make sure that information is:

- Fairly and lawfully and transparently processed;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and kept up to date;
- Not kept for longer than is necessary;
- Processed in a manner that ensures appropriate security of personal data.

Handling (also referred to as processing) means obtaining, recording, deleting, discussing or holding the data or doing anything to the data.

Any individual has the right to see personal information they are entitled to as well as other rights (see below for further details).

If individuals have any complaints as to how their information has been handled, they can contact the Information Commissioner's Office (ICO) to help.

How do I identify personal information?

If there is any doubt as to whether you are working with personal information, then ask yourself the following questions:

- Can a living individual be identified from the information or from the data and other information in the possession of or likely to come into the possession of, the Commissioner?

- Does the information 'relate to' the identifiable living individual, whether in personal or family life, business or profession?
- Is the information 'obviously about' a particular individual?
- Is the information 'linked to' an individual so that it provides particular information about that individual?
- Does the information have any biographical significance in relation to the individual?
- Does the information focus or concentrate on the individual as its central theme rather than on some other person, or some object, transaction or event?
- Does the information impact or have the potential to impact on an individual, whether in a personal, family, business or professional capacity?

If the answer is yes to any of the above, the data is likely to be personal information and the Data Protection legislation applies to it.

Special Categories of personal data

Certain types of data are defined as being special category personal data, for example information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, the processing of genetic data, biometric data for the purposes of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

Additional rules must be adhered to when processing such data and we will need a lawful ground for processing such data.

Criminal records and convictions information are now treated separately but additional safeguards are required to be put in place when processing such data.

How does the Commissioner use personal information?

The Commissioner collects and uses personal information about its staff and service users to allow it to perform its functions, to conduct its business activities, and comply with regulatory requirements, as well as to monitor the effectiveness of its services and policies.

Lawful basis for processing

The Commissioner can only process personal data if there are lawful grounds for doing so. This means:

- It is necessary for the performance of a contract with the individual or to take steps preparatory to such contract;
- It is necessary for the purposes of legitimate interests;
- It is necessary to comply with a legal obligation;
- It is necessary to protect the vital interests of a individual or another person where the data subject is incapable of giving consent;
- It is necessary to perform a public task in the public interest;
- With the consent of individual (which will be harder to obtain under GDPR).

If the Commissioner want to process sensitive personal data (special categories of data), the Commissioner can only process that data if we establish a second lawful ground for doing so i.e. in addition to those listed above. This means the Commissioner must satisfy at least one of the following conditions:

- Consent: the individual which must be explicit;
- Employment: the processing is necessary for carrying out obligations under employment, social security or social protection law;
- Vital interests: the processing is necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- Non-profit-body: the processing members' and former members' personal data by a non-profit body for political, philosophical, religious aims:
- Made public: the processing relates to personal data made public by the data subject;
- Legal claims: the processing is necessary for establishing, exercising or defending legal claims;
- Public interest: the processing is necessary for reasons of substantial public interest, based on EU or member state law;
- Health: the processing is necessary for preventative or occupational medicine; assessment of the working capacity of the employee; medical diagnosis; the provision of health or social care or treatment; or the management of heath or social care systems and services; and in all cases the processing is carried out by a health professional;
- Public health; the processing is necessary for the reasons of public interest in the area of public

health such as protecting cross –border threats to heath and ensuring high standards of healthcare;

- Archiving, research and statistics; the processing is in the public interest or scientific and historical research purposes.

Our legal obligations

The Data Protection legislation does not guarantee personal privacy at all costs, but aims to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal information. It applies to paper records as well as computer records.

This short checklist will help you comply with the Data Protection legislation. Being able to answer 'yes' to every question does not guarantee compliance, and you may need more advice in particular areas, but it should mean that you are heading in the right direction:

- Do I really need this information about an individual? Do I know what I'm going to use it for? Am I satisfied that I have a lawful basis for processing?
- Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?
- If I'm asked to pass on personal information, would the people about whom I hold information expect me to do this?
- Am I satisfied the information is being held securely, whether it's on paper or on computer?
- Is access to personal information limited to those with a strict need to know?
- Am I sure the personal information is accurate and up to date?
- Do I delete or destroy personal information as soon as I have no more need for it?

What is meant by a breach of the Data Protection legislation?

A 'personal data breach' is defined in Article 4(12) of the GDPR as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

These guidelines set out what may be considered a breach should you have access to or use personal information (it is not an exhaustive list).

Providing these guidelines are followed, the risk of any breach of the Data Protection legislation happening should be reduced:

- The transfer of personal information via email to external addresses, if the data is not encrypted.
- Copying personal information to CD-ROMS, laptops and/or other portable media without encryption which is then lost.
- Passing personal information to organisations, companies, or individuals who have not been declared as users of the information on behalf of the Commissioner to the person the information is about.
- The keeping of information which is no longer of value to, or applicable to, the Commissioner's activities.
- Deliberately changing information so that it is false.
- The loss of personal information, no matter how much content.

Please be aware that this is not a full list of breaches and further advice can be provided by the Data Protection Officer.

What if a breach occurs?

Overall responsibility for information security arrangements resides with the Commissioner .The Data Protection Officer should be made aware

of any suspected breaches and will investigate any potential breaches and report where required to the ICO.

Please familiarise yourself with the "How to handle an information security breach" policy. If you suspect a breach, please follow the procedure set out in that policy.

Staff responsibilities

A breach of the Data Protection legislation may have serious consequences for both the Commissioner and individuals, who fail to comply. It is therefore essential that staff comply with the following requirements at all times:

- Personal information may only be used for the purpose it was provided to the Commissioner or her staff for, as understood by the person providing that information. That is, to meet the business purposes of the Commissioner. To pass the information onto any party not employed through the Commissioner for any other purpose could result in a complaint and place us in breach of the Data Protection legislation. Please seek further advice from the Data Protection Officer if you wish to use personal information for purposes other than for which it was originally obtained.
- Security procedures must be complied with at all times, ensuring the confidentiality and security of any personal information that you have access to or use in the course of your work. See our Information Management Policy and our ICT Acceptable Use Policy to ensure that you follow the correct procedures.
- Care must be taken to ensure that information is accurate, appropriate and kept up to date.
- If asked to provide personal information, consider whether the applicant is entitled to the information. Seek advice from the Data Protection Officer if such enquiries are from outside the Commissioner's office.

- Any breaches of the Act must be reported to the Data Protection Officer.

All staff shall comply with information management procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

Housekeeping and Data Deletion

Pursuant to GDPR the Commissioner need to take steps to ensure that it is not keeping personal data longer than is necessary.

This is an important principle of existing data protection law and will be more rigorously enforced under GDPR.

This will mean that staff will need to carry out some housekeeping and delete data (which will include personal data) that it is no longer necessary to keep.

Whenever deleting data, staff should ensure that it does so securely and in accordance with the Records Management Procedures.

Subject access requests and other rights

Staff and members of the public may wish to access their or their relatives' personal information. Requests for access to personal information, from both internal and external sources, should be passed to the Data Protection Officer immediately.

The GDPR also provides the following rights for individuals:

- The right to be informed
- The right to rectification
- The right to erase
- The right to restrict processing
- The right to data portability
- The right to object

- Rights in relation to automated decision making and profiling

Please see the data subject request policy for further details.

Related Policies and documents

Information Management Policy
Records Management Procedures
ICT Acceptable Use Policy
Access to Information Policy
How to handle data subject requests
How to handle requests for information
How to handle an information security breach

Older People's Commissioner for Wales
Comisiynydd Pobl Hŷn Cymru

Appendix 1