Comisiynydd Cenedlaethau'r Dyfodol Cymru
Future Generations Commissioner for Wales

Internal

Data Protection Policy

Policy Statement

The Future Generations Commissioner is committed to ensuring that information is well managed according to best practice standards and in compliance with the Commissioner's legal duties under the Data Protection Act (DPA) and General Data Protection Regulation (GDPR) and Privacy and Electronic Communications Regulations (PECR).

The GDPR comes into effect on 25th May 2018; a new Data Protection Act should come into law during 2018. The changes to data protection regulation have required that we review and amend our approach to managing personal information.

This policy applies to our use of personal information i.e. information that identifies or is about a living individual. As a public body good information management is a matter of public trust; we have a responsibility to protect the personal data that we hold and to process and share it lawfully.

Responsibilities

The Commissioner expects that all staff and associates comply with the requirements of this policy.

Director of Finance and Corporate Governance (Helen Verity) has broad responsibility for Data Protection and is the named Data Controller.

The GDPR requires that we designate a Data Protection Officer.
Our DPO is Sang-Jin Park; the DPO will monitor day to day compliance, providing advice and guidance to staff on DP and privacy issues. The DPO also responsibile for our communication with the Information Commissioner's Office (ICO) concerning notification of processing, data loss or breach and complaints.

The Audit Committee retains oversight of DP compliance. Any DP issues are discussed (as a standing item) at ARAC meetings on quarterly basis

Demonstrating Compliance

To ensure our continuing compliance with data protection and GDPR have taken the following steps:

- We have implemented appropriate technical and organisational measures that ensure and demonstrate that we comply. This includes our review of information governance policies and processing activities, internal audits, reviews of internal HR policies and procedures, and staff training.

- We maintain relevant documentation on our processing activities.

- We have designated a data protection officer

- We have implemented a 'privacy by design' approach

Data Protection Principles

The GDPR Principles are similar to the original 8 Data Protection Principles and are included in full at Appendix A. The GDPR specifies that the Data Controller is responsible for compliance with these principles.

In brief the GDPR Principles state that personal data shall be:

- processed lawfully and fairly in a transparent manner to individuals concerned
- 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 the purpose for which they are processed
- accurate and kept up to date; incorrect information to be erased or rectified without delay
- 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
- appropriate technical and organisational measures applied to safeguard the rights and freedoms of individuals
- processed securely and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Key Definitions

Data Subject – the individual who is the subject of the data

Data Controller – determines the purposes and the means of processing the data

Data Processor – is responsible for processing personal data on behalf of the controller

Personal data - any information relating to an identifiable person (data subject), this can include the obvious names and addresses as well as email addresses and images.

Special category data (sensitive personal data)

- Special category data is more sensitive so requires a greater degree of protection.
- This includes information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.
- A loss or breach of this type of data could create more significant risks to a person's fundamental rights or freedoms, e.g. putting them at risk of discrimination.
- To process special category data we must satisfy certain conditions of the GDPR.

Privacy by Design and Data Protection Privacy Impact Assessments (DPIA)
We have an obligation to implement measures (technical and organisational) to show we have considered and integrated data protection into our processing activities. For example, at the planning stages of a new partnership project we will consider DP issues. Complex projects may require a Data Protection Privacy Impact Assessment (DPIA). Our DPO will advise when this is required.

Further information is included as Appendix C

Data Sharing Agreements may be appropriate in particular circumstances and the Wales Accord for Sharing Personal Information (WASPI) provides a template that can be adapted where a number of organisations wish to share personal information. Our DPO can advise when this may be appropriate and on adapting the template.

Lawful basis for processing – we must have identified a valid lawful basis for any processing before processing begins. For example, one lawful basis is consent however, the GDPR sets a high standard for consent and we should consider whether other basis for processing are more appropriate.

Individual Rights
A data protection approach relies on us to fulfil the responsibilities and obligations of

a data controller. We need to be mindful of the rights and freedoms of individuals as we carry out our work. The GDPR extends an individual's rights in relation to their data; a full explanation of these rights is included in Appendix D.

However, these are the most relevant to us:

Right to be informed – we must tell individuals about our processing of their data and how to contact us to exercise their rights. We use a Privacy Notice to do this.

Right of access – this gives individuals the right to a copy of the data we hold and is also known as 'subject access request'.

Rights to rectification (correction or completion of inaccurate personal data), erasure (also known as the right to be forgotten) and the right to object to processing or for processing to be restricted.

We must provide a response to a rights request within **20 days**.

Data Loss and Breaches

Through our Information Governance policies and procedures we have established a framework for good information handling. We have put in place the technical and organisational measures to appropriately protect the personal data that we hold.

However, the risk of a security incident that affects the confidentiality, integrity or availability of personal data remains. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data. This includes breaches that are the result of deliberate and accidental causes.

It is vital therefore that you are aware of your responsibility to report a potential data loss or breach immediately you become aware of it.

Personal data breaches can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction)
- Sending personal data to an incorrect recipient
- Devices containing personal data being lost or stolen
- Alteration of personal data without permission

- Loss of availability of personal data

The GDPR places a duty on organisations to report certain types of personal data breach to the ICO within 72 hours and should the breach significantly impact on individuals we must inform them without delay. An organisation maybe fined significant amounts for serious breaches and for failure to report a breach as required.

Working with IT Support Orbits IT, we have put in place robust breach detection.

Our Data Breach/Loss Policy details the steps we must take should a breach or loss occur.

We have allocated responsibility for investigation of potential breaches or loss to the DPO.

Privacy and Electronic Communications Regulations (PECR)

PECR works alongside data protection and is cover electronic marketing activity by phone, fax, email, text or any other type of electronic mail. GDPR does not replace PECR and we need to comply with both in any direct marketing activity.

Protecting Personal Information - Do's and Don'ts

Do – familiarise yourself with the GDPR principles

Do – familiarise yourself with individual rights under GDPR – they are your rights too.

Do – consider privacy issues as part of your initial project design

Do –think about lawful basis for any processing of personal data before you begin processing

Do – think about your day-to-day activities and where privacy risks may arise e.g. do you routinely forward emails without checking with email originator first?

Do – seek advice from the DPO at an early stage

Don't - share personal information if you are in any doubt that you are safe to do so. Check with the DPO and make sure you are complying with GDPR.

Don't - delay reporting a problem – a potential loss or breach. Early reporting can prevent an issue getting worse.

Sources of Advice and Guidance

Our Data Protection Officer (DPO) can provide advice and guidance in relation to day to day data protection compliance issues.

The Information Commissioner's Office has published and continues to update detailed guidance on GDPR compliance.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Related Policies

Information Governance Policy

IT Security & Acceptable Use Policy

Information Security Policy

Freedom of Information (FOI) & Environmental Regulations Policy

Access to Information Guidance

Data Breach Policy

Appendix A: GDPR Principles

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that:
- the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Appendix B - Managing a Request for Personal Information (SAR) Procedure

- Record request received
- Pass to DPO
- Open file and apply unique reference number
- Identify respond by date – 20 days from receipt
- Clarify request - scope
- Identity check
- All staff email with response date
- Collate information
- Check 3rd party content
- Prepare response to data subject
- Content check
- Response to data subject within 20 days

Responding to other rights based requests

- Record request
- Pass to DPO
- Open file and apply unique reference number
- Identity check
- Identify information/processing
- Clarify request if necessary
- Carryout correction/deletion
- Record action
- Confirm to data subject action carried out
- File closed

Appendix C – Privacy by Design Principles

1. The approach must adopt a proactive rather than reactive stance and aim at preventing privacy risks and not at addressing them after they occur
2. Privacy is to be used as a default setting
3. Privacy must be embedded into design
4. Privacy by Design ensures full functionality and seeks to achieve both privacy and security
5. Security must be made an integral part of the systems throughout their whole lifecycle
6. It seeks to achieve visibility and transparency

7. Systems are to be kept user-centric and users interests and needs must be taken into account.

Appendix D - Individual Rights under GDPR

Right to be informed - Individuals have a right to be informed about the collection and use of their data. This is a key transparency requirement under the GDPR. We use a Privacy Notice to do this.

Right of access – individuals have a right of access to their personal data. This right allow individuals to be aware of and to verify the lawfulness of the processing.

Right to rectification – individuals have the right to have inaccurate personal data rectified or completed if it is incomplete.

Right to erasure – individuals have a right to have their personal data erased (also known as the right to be forgotten). This right is not absolute and only applies in certain circumstances.

Right to restrict processing – individuals have the right to request the restriction or suppression of processing of their personal data. This right is not absolute and only applies in certain circumstances.

Right to data portability – This right allows individuals to obtain and reuse their personal data for their own use across different services.

Right to object – individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest; direct marketing and processing for purposes of scientific/historical research and statistics.

Rights related to automated decision making and profiling – individuals subject to this type of processing must be given information about the processing and simple ways to request human intervention or challenge a decision.