Ymddiriedolaeth Ddiwylliannol Cultural Trust

awen Masnachu Trading

GDPR Guidance and Responsibilities

A brief overview and your responsibilities in relation to the General Data Protection Regulations (GDPR).

Contents

WHAT IS DATA PROTECTION LAW?

GDPR came into force on the 25th May 2018 and is part of the Data Protection Act 2018.

Since Brexit, the UK has continued to apply the data protection acts 1998 & 2018 to set out how data is used and processed. Everyone responsible for handling and using this data has to follow strict rules called 'data protection principles'. The law only applies to information that ***identifies a living individual.***

The Data Protection and Digital Information Bill, was introduced to parliament in March 2023. It is the product of a major consultation the government held last year on reforming the UK GDPR and other privacy legislation following Brexit. Until the bill becomes law Awen must continue to comply with GDPR 2018.

WHAT IS PERSONAL DATA?

Information that on its own (or with other available data) can identify an individual.

GDPR applies to 'personal data'; meaning any information relating to an identifiable living person who can be directly or indirectly identified by it.

This definition provides for a wide range of personal identifiers to constitute personal data, including: **name**, **identification number**, **location data** or **an online identifier**.

This reflects changes in technology and the ways in which organisations collect and hold information about people.

WHAT IS 'SENSITIVE' PERSONAL DATA?

Some categories of personal data are considered particularly sensitive and require additional protections.

What are the special categories of data?

The law says there are certain types of personal data that have a higher sensitivity, and where an organisation holds this data, there is a higher risk to a person's rights as a result. Therefore, this data must have a higher level of security. This is data about an individual's:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs, or;
- Trade union membership, and the processing of;
- Genetic data;
- Biometric data;
- Mental or physical health;
- Sex life or sexual orientation.

WHAT ARE YOUR RESPONSIBILITIES?

- Complete all training and read and sign to confirm your understanding of the policy and relevant procedures.
- Only process data if you are required to do so as part of your role.
- Only collect the data you are required to for that transaction. Do not collect data if it is not necessary.
- Ensure personal data security - Locked cabinets, lock computer screens, confidentially dispose of documents which contain personal data, don't leave personal data on desks visible in working areas.
- If you become aware of data not being stored securely make someone aware of it.
- If you become aware of a personal data breach or possible data breach, report it to the Data Protection Officer (DPO) immediately.
- Do not provide personal data unless you are permitted to do so. Third party requests should always be sent to the DPO. This includes requests for CCTV images.
- Only keep records for as long as they are required. Refer to Retention Policy. If you are unsure speak to your Manager or contact the DPO.
- In customer facing roles, frequently check data held with the customer to ensure personal data is up to date.
- If you are creating a new form that collects personal data, please seek advice from the DPO before use.
- If you are unsure don't assume always ask for advice before sharing or processing data.

DATA PROTECTION PRINCIPLES

The seven rules that Awen must follow in order to comply with the law.

Awen is required by law to ensure that personal data is used fairly and lawfully, and GDPR holds a set of principles which describe how such data should be handled:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and, where necessary, kept up to date;
- Kept for no longer than is necessary;
- Ensures appropriate security;
- Demonstrate compliance with the principles.

ENFORCING THE LAW

The UK regulator is the Information Commissioners Office (ICO). The public can complain about Awen to this body. The ICO can investigate and has a range of powers including the ability to fine.

Data Protection legislation is regulated in the UK by the Information Commissioner's Office (ICO). The ICO are the UK's independent authority set up to uphold information rights in the public interest; promoting openness by public bodies and data privacy for individuals.

The ICO provides Codes of Practice, advice and guidance to organisations to enable their compliance with legislation and they have the power to take enforcement action when things go wrong. These powers include:

- Information Notices – requiring that organisations tell the ICO about their practices
- Decision Notices – published written judgements on the outcome of an investigation
- Enforcement Notices – legal orders requiring organisations to make specific improvements
- Monitoring – Making sure an organisation improves over time
- Consensual or compulsory audits – Investigations into practices through on-site audits
- Monetary Penalties – Fines of up to €20,000,000

INFORMATION GOVERNANCE FRAMEWORK

Awen must identify key roles and responsibilities to make sure we comply with the law.

In order to manage personal information lawfully and fairly it is essential that Awen identifies roles and responsibilities to support this.

All staff have responsibilities to ensure they know who to go to for advice on Data Protection issues.

Compliance with legislation must be documented and evidenced on a continual basis in order to comply with Data Protection Principle 7.

DATA PROTECTION OFFICER ROLE

Monitors internal compliance, informs and advises on data protection obligations, Privacy Impact Assessments and is a point of contact for staff on data protection matters.

Awen's DPO is the Head of People who's role is to:

- Ensure awareness and training is in place for employees and regularly completed/ reviewed
- First point of contact for Data Subjects in relation to queries on how their data is handled
- First point of contact with the ICO for regulatory matters
- Approves Information Sharing Agreements
- Approves Privacy Impact Assessments
- Ensures adequate reporting to senior leaders on compliance with information management

The role of DPO can be carried out in conjunction with another role, provided there is no conflict of interest; shared with other organisations, or contracted-out.

PRIVACY NOTICES & CONSENT

Is directed externally. It explains to clients, customers, website visitors, authorities, and other interested parties what Awen does with personal data.

The law requires Awen to process personal information fairly and lawfully and in a transparent manner.

FAIRLY – if an individual does not have a clear understanding of how we are using their information, or how to exercise their rights, then it cannot be considered 'fair'. Awen must make available at the point of collection a privacy notice explaining to individuals:

- Why their data is used;
- How it is secured;
- How long it is kept;
- Who we will share it with;
- How to exercise their rights;
- How to contact the Data Protection Officer;
- The legal basis for the processing of their information.

LAWFULLY – there must be a clear and documented legal basis for Awen to process personal information about an individual. There are a number of legal permissions we can use, including:

- Consent (e.g. customer consent to receive marketing emails);
- Required by law (eg. criminal investigation);
- Entering into a contract (eg. your contract of employment);
- Vital interests (in order to protect health in emergencies);
- Public tasks in the public interest (eg. holding CCTV or visitor data for security).

THE RIGHTS

Data subjects have eight rights under GDPR.

GDPR provides a number of rights in relation to how personal information is used to ensure that processing is fair. These rights include:

- Right to be informed
- Right of Access
- Right to Rectification
- Right to Erasure
- Right to Restriction
- Data Portability
- Right to Object
- Rights related to Automated Decision Making & Profiling

Any staff member receiving a request to exercise these rights, which may be in writing or verbally, should immediately make the Data Protection Officer aware of the request to ensure it is handled within the legal timescales (a calendar month).

REQUESTS FOR INFORMATION

We must have procedures in place for dealing with requests for personal data so that we can fulfil them within legal deadlines.

GDPR provides a right of Access to information, known as Subject Access Requests.

Individuals can request access to personal data about them held by Awen. We must therefore ensure we only provide personal data to individuals who have a legal right to it. This involves checks of ID, and potentially removing certain information from the records disclosed.

INFORMATION SHARING

We must only share data with other bodies where the laws allows us to, or with an individual's consent.

Any sharing of personal data outside of Awen should be documented. Remember, unless the law requires us to share, we cannot do so without the individual's consent.

In circumstances where the law does require us to share (and we therefore do not need to seek consent), we must still ensure that our privacy notice advises individuals of the circumstances where we may share their data.

Any sharing of sensitive data must be documented in a relevant system, detailing:

- The date of sharing
- The information shared
- Who you shared the information with
- Your rationale for deciding to share the information

If the sharing is intended to be regular, it must be supported either by a contract or an information sharing protocol to ensure the correct security arrangements are in place.

PRIVACY BY DESIGN & DEFAULT

We must understand the risks of how we manage personal data, undertaking statutory risk assessments where necessary.

A key mechanism for assessing risk is the Data Protection Impact Assessment (DPIA).

The DPIA will document what you want to do, the data you wish to use, the legal basis, how the data will be secured and managed and how individuals can exercise their rights in relation to the processing. If there is a risk to people's rights from our activities, the law says we must conduct a DPIA, and our DPO must approve it.

BREACH MANAGEMENT

Where we have incidents of data being lost, stolen, given to the wrong person or deleted when it shouldn't have been, staff must report it to the DPO and it must be investigated. Decisions need to be made about reporting to the ICO within 72 hours.

Under GDPR there is a legal requirement to notify the ICO of any serious breaches involving personal data within **72 HOURS**.

It is therefore important that you understand your responsibilities including how to identify a breach, who to report incidents to, and ensuring all staff are trained on how to use technology securely and effectively in line with their role.

When a serious breach occurs we will be required to consider notification to the affected individuals. If we take the decision not to inform them, the ICO may overrule that decision if they feel it is in the best interests of the individuals.

The UK GDPR and DPA 2018 set a maximum fine of £17.5 million or 4% of annual global turnover – whichever is greater – for infringements.

FURTHER INFORMATION

For further information, please visit **https://ico.org.uk/**

Ymddiriedolaeth Ddiwylliannol Cultural Trust

awen Masnachu Trading

Ymddiriedolaeth Ddiwylliannol Awen
Swyddfeydd y Stablau, Tŷ Bryngarw,
Brynmenyn, Pen-y-Bont, CF32 8UU

Awen Cultural Trust
Stable Offices, Bryngarw House,
Brynmenyn, Bridgend, CF32 8UU

+44 (0) 1656 754825
enquiries@awen-wales.com
www.awen-wales.com

Rhif elusen gofrestredig / Registered charity number: 1166908
Rhif cofrestru TAW / VAT registration number: 224 3341 44
Rhif gofrestredig / Company number: 9610991