Un Llais Cymru
One Voice Wales

Community & Town Councils Digital Guidance

Data Protection Considerations

March 2025

Contents

Introduction

Community and Town Councils in Wales should implement a robust data protection approach to keep information private and secure. Data protection includes practices and rules to safeguard personal data and ensure privacy rights.

A solid data protection policy is essential for Community and Town Councils. It provides a system for handling data responsibly and helps establish resident trust. It also ensures Councils comply with relevant laws such as the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018. These laws set strict rules on how to collect, use, store, and share personal data, with penalties for non-compliance.

Key aspects of data protection laws in the UK include transparency in using personal data and ensuring its security. Councils need to employ suitable technical approaches and regularly train staff on data protection.

Benefits

Community and town Councils in Wales can reap numerous advantages by instituting a robust data protection policy. These benefits span across legal, operational, and reputational aspects, ensuring that Councils not only comply with legislation but also cultivate trust and efficiency within their operations.

Legal Compliance

One of the primary benefits is ensuring compliance with the General Data Protection Regulation (GDPR). By adhering to these regulations, Councils can avoid hefty fines and legal repercussions associated with data breaches and non-compliance. This regulatory alignment further facilitates smoother interactions with regulatory bodies and enhances overall governance.

Enhanced Trust and Reputation

A well-articulated data protection policy signals to the community that the council is committed to safeguarding personal information. This commitment fosters trust among residents and stakeholders, reinforcing the council's reputation as a responsible and transparent entity. Trust is critical in maintaining positive community relations and ensuring active participation in council initiatives.

Risk Mitigation

A comprehensive data protection policy helps identify and mitigate potential risks associated with data handling and processing. By conducting regular Data Protection Impact Assessments (DPIAs), Councils can proactively address vulnerabilities and

implement necessary safeguards to protect personal data from breaches or unauthorized access.

Data Subject Rights

A robust policy ensures that the rights of individuals, such as the right to access, rectification, and erasure of their data, are upheld. This not only aligns with legal requirements but also demonstrates the council's dedication to respecting and protecting the personal information of its constituents.

Increased Awareness and Training

Developing and maintaining a data protection policy necessitates continuous staff training and awareness programs. These initiatives ensure that all council members are knowledgeable about data protection principles and practices, fostering a culture of data privacy and security within the organization.

Key Terms and Concepts of Data Protection

1. Personal Data

Personal data refers to any information relating to an identifiable person who can be directly or indirectly identified. This includes names, email addresses, identification numbers, location data, and online identifiers.

2. Data Processing

Processing encompasses any operation or set of operations performed on personal data. This includes collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction of data.

3. Data Controller

A data controller is a person, public authority, agency, or other body that determines the purposes and means of the processing of personal data. They are responsible for ensuring compliance with data protection laws.

4. Data Processor

A data processor is a person, public authority, agency, or other body that processes personal data on behalf of the controller. They must act on the documented instructions of the controller and implement appropriate security measures.

5. Consent

Consent means any freely given, specific, informed, and unambiguous indication of the data subject’s wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of their personal data.

6. Data Subject Rights

Data subjects have several rights under the GDPR, including the right to access their data, the right to rectification, the right to erasure (also known as the right to be forgotten), the right to restrict processing, the right to data portability, and the right to object to processing.

7. Data Protection Impact Assessments (DPIA)

A DPIA is a process to help identify and minimize the data protection risks of a project. It is required in situations where data processing is likely to result in high risk to individuals' data protection rights. Community Councils must conduct DPIAs for projects that are likely to result in high risks to individuals' data protection rights. A DPIA helps identify and minimize data protection risks.

8. Data Breach

A data breach is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. Community Councils should have procedures in place to handle data breaches promptly and effectively.

9. Data Protection Officer (DPO)

A DPO is an individual appointed to ensure that an organization is complying with the laws protecting individual's data. They are responsible for overseeing the data protection strategy and its implementation to ensure compliance with GDPR requirements.

10. Privacy by Design and by Default

This concept requires data protection to be included from the onset of designing systems, rather than as an addition. It ensures that data protection is built into the development of business processes for products and services.

Summary of the GDPR UK

The General Data Protection Regulation (GDPR) UK framework provides a robust set of requirements for community Councils in Wales to protect individuals' personal data. Community Councils must adhere to several key principles and rights under GDPR to ensure compliance.

Key Rights

Community Councils must respect and facilitate data subjects' rights, which include:

- The right to access their data
- The right to rectification of any inaccuracies

- The right to erasure, also known as the right to be forgotten
- The right to restrict processing of their data
- The right to data portability
- The right to object to data processing

One Voice Wales members have access to resources around data issues, including guidance on GDPR and model templates for data access requests, to support compliance with these regulations.

Version History

	Date	Issuer	Reason	Review Date
V1	13/03/25	Justin Horrell	Initial Version	13/03/26

Ariennir gan
Lywodraeth Cymru
Funded by
Welsh Government