

Welshampton and Lyneal Parish Council

Report to Council May 2018 General Data Protection Regulations (GDPR)

Purpose of Report

This report is to update the Parish Council on the GDPR, which come into force on 25 May 2018 and replace the existing law, the Data Protection Act 1998. Local Councils must comply and arrange for the control of personal data held and processed by the Council (the Data Controller).

Introduction

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), so if complying properly with the current law means most of the approach to compliance will remain valid under the GDPR and can be the starting point to build from. However, there are new elements and significant enhancements, so some new processes and procedures will need to be implemented and some existing processes and procedures will need to be amended or enhanced. To gain a good understanding of GDPR Councillors are asked to read the NALC's 'A GDPR Toolkit for local councils'.

Please note although a 62-page document the main sections are contained within the first 25 pages

GDPR Principles

Under the GDPR, the data protection principles set out the main responsibilities.

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"

Clerk: Carole Warner,
Orchard Cottage,
Rowe Lane,
Welshampton,
Ellesmere, SY12 0QB
Tel. 01948 710672
email: clerk@welshamptonandlyneal-pc.gov.uk
www.welshamptonandlyneal-pc.gov.uk



Accountability and Governance

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance.

Comprehensive but proportionate governance measures are expected to be put into place. This will mean more policies and procedures building on good governance measures already in place.

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Key Areas to Consider

- Lawful processing

The lawful basis for processing personal data must be identified, documented and any privacy notice updated to explain it. Under the current law the lawful basis for processing personal data does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on the lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where consent is used rather than a contract or a legal obligation as the lawful basis for processing.

- Consent

How consent is sought, recorded and managed must be reviewed and any changes for GDPR made. Currently the Parish Council does not need to seek consent. In most circumstances residents contact the Parish Council for assistance/information rather than the Council contacting the resident. Processing is likely to come under the lawful basis of public interest ie processing is necessary for the performance of tasks carried out by a public authority.

- Individual rights

The GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

- Subject access requests

Procedures should be reviewed in order to manage requests under GDPR:

- In most cases there is no charge payable for complying with a request.
- There will be one month to comply, rather than the current 40 days.
- Requests can be refused or charged that are manifestly unfounded or excessive.
- If a request is refused, the individual must be told why and that they have the right to complain to the supervisory authority and to a judicial remedy. This must be done without undue delay and at the latest, within one month.

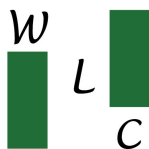
Day to day processes and record management procedures need to be reviewed.

- Personal Data Breaches

The right procedures must be in place to detect, report and investigate a personal data breach.

- Data Protection Officer (DPO)

The GDPR introduces a duty for public authorities to appoint a (DPO). DPOs assist the Council by monitoring internal compliance, informing and advising on protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs) and acting as a contact point for the ICO.



Welshampton and Lyneal Parish Council

The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level ie Parish Council.

Discussion on who can be a DPO for Parish Councils is still being carried out by ICO. There is no necessity to appoint a DPO at this stage.

Until this is resolved and to provide central support and guidance in respect of compliance with the GDPR, the Council should consider the appointment of the Clerk as Data Protection Compliance Officer in order that steps towards compliance can be achieved.

Other Areas

Other areas covered by the GDPR include:

- Personal data of children – the Council does not collect data of children
- Data protection by design and data protection impact statement – the volume and level of data collected by the Council does not currently warrant this.
- International processing – the Council only operates in one country.

Working toward compliance

The following High Level Action Plan sets out the basic documentation that should be put in place to demonstrate that the Council is working towards compliance. A detailed Action Plan will be maintained by the Clerk in order that progress can be monitored.

High Level Action Plan		
Document	Detail	Comments
Data audit and lawful basis for processing	What data is held? Where does it come from? Where is it kept and who has access? What does the Council do with it? Who is it disclosed to? What lawful basis is collected by? What security measures are in place.	<i>Documents and records should be retained no longer than necessary.</i>
Privacy Notice(s)	Must be transparent and clear in plain language, easy to access	<i>Two-tiered approach: Summary on documents and emails Detailed privacy notices to be held on website</i>
Consent Forms	Must be by 'opt in' method and appropriate	<i>On receipt record how and when consent is obtained</i>
Data Processing Log	To include: Subject matter Duration Nature and purpose of processing Type of data	<i>Data Audit document to be expanded to include this information.</i>

Clerk: Carole Warner,
Orchard Cottage,
Rowe Lane,
Welshampton,
Ellesmere, SY12 0QB
Tel. 01948 710672
email: clerk@welshamptonandlyneal-pc.gov.uk
www.welshamptonandlyneal-pc.gov.uk



High Level Action Plan		
Document	Detail	Comments
	Categories Retention duration	
Policies/Procedures		Comments
Data Protection Policy		<i>Reviewed April 2018</i>
Email Acceptable Use Policy		<i>Review</i>
Record Management Policy		<i>Review</i>
Date Subject Access Request Policy		<i>New Sample response letters to be prepared</i>
Breach Procedure		<i>New</i>
Social Media Policy		<i>Review</i>
Management of Transferable Data Policy		<i>New</i>

It is possible that not all recommended documentation will be completed by 25 May, but the detailed Action Plan will show what plans the Council has in place to complete the remaining/ongoing steps.

Recommendations:

1. The Council endorses the High Level Action Plan set out above and notes the detail set out in NALC's 'A GDPR Toolkit for local councils'
2. The Council adopts the following documents:
Information and Data Protection Policy
Privacy Notice (Councillors, Staff and Role Holders)
Privacy Notice (General)
Consent to hold Contact Information
3. The Council appoints the Clerk as Data Protection Compliance Officer and delegates responsibility for completing audits and drafting for approval the necessary documentation under the GDPR.
4. The Council will address the appointment of a DPO once options are further clarified.

Carole Warner
23 April 2018