

Huggate Parish Council

General Data Protection Regulations

Introduction

The regulation known as General Data Protection Regulation (GDPR) will come into force on 25 May 2018. The UK Government will introduce new legislation to repeal the Data Protection Act 1998 and to ensure that new UK legislation does not create inconsistencies with the GDPR.

The purpose of this paper is to provide background information to councillors and to enable a discussion on the Parish Council's preparations for the introduction of GDPR.

Purpose of GDPR

GDPR builds on the legal framework established by the 1998 Data Protection Act to balance the needs of organisations (businesses, not-for-profits and public bodies), in their capacities as data controllers and data processors to collect and use personal data, against the rights of an individual to have their information (personal data) kept secure and private.

GDPR has been introduced to address the privacy issues arising from a digital age in which personal data may be collected, transmitted, stored, manipulated and shared with relative ease eg. using emails, websites, the internet and the cloud. The purpose is to increase (i) the obligations on organisations when acting as data controllers and (ii) the rights of individuals to ensure that their personal data is respected and used only for legitimate purposes.

Implications for the Parish Council

The major impact for the Parish Council will be the need to have documentation to demonstrate its accountability in respect of data protection. Many things the Council is doing already comply with the current Data Protection Act. 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;
- The right not to be subject to automated decision-making including profiling.

Lots of the concerns and implications for larger organisations are connected with the automatic processing of data. Although the Parish Council holds personal data on computer systems, there is very little automatic processing involved.

Practical steps the Parish Council will need to take

1. When the Parish Council requests or receives any personal data it should issue a privacy notice setting out: the Parish Council identity, how it intends to use the information, the lawful basis for processing the data, the Council's data retention period and the fact that individuals have a right to complain to the Information Commissioner's Office if they think there is a problem with the way the council is handling their data. This privacy notice must be provided in concise, easy to understand and clear language. The Parish Council must have a Subject Access Request (SAR) procedure (see below for Clerks email to contact to request a SAR setting out how it will handle any request from an individual about the data it holds on them.

2. The Parish Council should prepare a document which describes the personal data it processes.

Personal data held by the Parish Council falls into the following eleven categories. Where information other than contact details is held, this is mentioned specifically:

- Electoral Register (including unique electoral identifier)
- Common Land Registration records
- Councillors' details (including Register of interests)
- Suppliers to the Parish Council (if individual, not corporate, including bank account details)
- External organisation contacts / Community organisations
- Contractors (where individuals can be identified rather than a corporate body)

- Employee (Clerk) (including National Insurance Number) • Business contacts (eg. CDALC, SLCC)

- Local residents / electors.

For each category of data, the following will be recorded:

- a. What data is held

- b. Where the data came from

- c. How the data was obtained / consent sought

- d. Why the data is needed

- e. The lawful basis for processing this data

- f. With whom the data is shared by the Parish Council

- g. What would constitute a data breach requiring notification to the ICO or affected individuals

A draft of such a document is provided at Appendix 1.

3. The Parish Council should prepare a consent mechanism for each of the above categories of data, using a checklist offered by the Information Commissioner's Office. Consent to hold an individual's data must be freely given, specific, informed and unambiguous. There must be a positive opt-in — consent cannot be inferred from silence, pre-ticked boxes or inactivity, and there must be a simple way for people to withdraw their consent.

4. As the Parish Council does not process any data for individuals under 16, specific systems to verify individuals' ages, other than 'over 16' will not be necessary.

5. The Parish Council needs a procedure in place to detect, report and investigate any personal data breach (failure to report a breach could result in a fine, as well as a fine for the breach itself).

Note that if 'consent' is given as the lawful basis for processing personal data then those individuals have a right to have their data deleted.

Data Protection Impact Assessment / Privacy Impact Assessment

Data Protection Impact Assessments are mandatory in certain circumstances where data processing is likely to result in high risk to individuals, for example: where a new technology is being deployed, where a profiling operation is likely to significantly affect individual, or where there is processing on a large scale. Data processing by the Parish Council is not considered to meet these criteria and therefore a Data Protection Impact Assessment is not necessary.

Appointment of Data Protection Officer

The Parish Council is no longer required to formally designate a Data Protection Officer (DPO). However it is agreed that should the need of a DPO be required then the role sits with the Chair and they should take responsibility for the Parish Council's data protection compliance and have the knowledge, support and authority to carry out their role effectively.

The minimum tasks of an organisation's DPO will be:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws;
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on impact assessments, train staff and conduct internal audits;
- If the need arises to be the first point of contact for the Information Commissioner's Office and for individuals whose data is processed. Whilst the DPO can be appointed from within an organisation or as an external data protection adviser, clear advice from the National Association of Local Councils is that a Parish Council's Clerk/RFO should NOT be designated as DPO, nor a councillor unless they have expert knowledge of data protection law and practices. Specifically, an 'internal' appointment (either Clerk or councillor) will not satisfy all of the requirements of the job because:
 - There are conflicts of interests (which may arise from responsibilities as a clerk/RFO and may including processing activities);
 - The need for independence;
 - The need for expert knowledge of data protection law and practices; and
 - The need for adequate time to perform DPO role.

Options if required are use one of the many reputable firms that understand the sector ('trusted suppliers') which council can then approach, or a supplier who provides a national service which local councils then buy into as their appointed DPO

General Data Protection Regulations
Huggate Parish Council

General Data Protection Regulation Impact Assessment / Personal data held by Huggate Parish Council

Category of Data	What Data is held	Where the data came from	How the date was obtained/consent sought	Why this data is needed	Lawful basis for processing this data (eg consent)	With whom the data is shared	What would constitute a data breach
Electoral Register for the parish	Name/Address Unique electoral identifier	ERYC	Through registration and provided by ERYC	Eligibility for election or co-option to the PC	Required on a month by month basis to support policies	Parish councillors and clerk only	Information visible to others
Common Land Registrations	Name/Address	ERYC	Correspondence	Only held for the village pond	Proof of ownership	Parish councillor only	N/A-no personal info held on documents
Councillors details	Name/Address/Email/Telephone numbers/ Register of interests	Parish Councillors	Paper proforma on election/co-option	Internal correspondence Public register of interests Access to councillors by the public	Required as part of councillors agreement and declaration	Within HPC, uploaded ERYC website	Transparent government relates
Supplier (if individual nor corporate)	Name/Address/telephone numbers/Bank account details	Business Correspondence	Business Correspondence	Business transactions	Required to purchase goods and services	Councillors and clerk only	Contacts/bank info given to other intentionally or unintentionally
External Organisations	Name/Address/telephone numbers	Ward Councillors, other clerks info	Provided by ERYC	Day to day business of HPC	Only used for contacted if needed	Councillors and clerk only	Transparent government relates

Employees	Name/Address/Email/telephone numbers/Ni No	Contact with the individual	Business Correspondence (mainly email)	To conduct PC business	Clerk and chair/vice chair only for wages etc	Chair and vice chair	Ni No & personal information given to others
Residents/electors within the parish	Name/Address/Email/telephone numbers	Letters, emails, webforms, telephone calls or completed surveys.	Incoming Correspondence	Engagement with the PC	Required for communication purposes with parishioners	Councillors and clerk	Contact details seen by none councillors and clerk

The following notice is given when personal data is collected by the Parish Council: Identity:

Huggate Parish Council Data controller: Abby Popely, the Clerk, Data Protection Officer for Huggate Parish Council: not required unless a security breach occurs or a complaint is received the Chair will take on the role

To be appointed Legal basis for using the information: Data retention period: see Data Protection Policy Retention Policy and Retention of documents

Right to complain: If you think there is a problem with the way we are handling your data, then you have a right to complain to the Information Commission.

The contact details are: 0303 123 1113 or email casework@ico.org.uk, alternatively the postal address is: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

What will happen if a data breach is identified: the Chair will take on the role of DPO to investigate any complaints or security breach.

Is a Data Protection Impact Assessment necessary: (if no, why not) International considerations: The Parish Council does not operate in more than one EU member state. Children: The Parish Council does not hold or process any data relating to children under the age of 16.