BARTHOMLEY PARISH COUNCIL

General Data Protection Regulation (GDPR)
May 2018

INTRODUCTION
Data protection law will change significantly on 25 May 2018, when the 2016 EU Directive known as the *General Data Protection Regulation (GDPR)* takes effect.

GDPR will replace the 1998 Data Protection Act. The UK's decision to leave the EU will not affect the commencement of the GDPR in 2018.

The Parish Clerk is already in the process of preparing for the new regulation and has attended training on GDPR.

The main concepts and principles of GDPR are very similar to the Data Protection Act 1998, but it will mean that the Parish Council needs a Data Protection Policy.

The Information Commissioner's Office (ICO) is adopting a 'light touch' regime in respect of local councils as they are not a high-risk sector; however, local councils are expected to have arrangements in place to comply with the Regulation, as soon after 25 May 2018 as practicable.

UNDERLYING PRINCIPLES
The underlying principles in GDPR include the provisions that personal data:

(a) Must be processed lawfully, fairly and transparently.
(b) Is only used for a specific processing purpose that the data subject has been made aware of and no other, without further consent.
(c) Should be adequate, relevant and limited, i.e. only be the minimum amount of data should be kept for specific processing.
(d) Must be accurate and where necessary kept up-to-date.
(e) Should not be stored for longer than is necessary and that storage is safe and secure.
(f) Should be processed in a manner which ensures appropriate security and protection.

NEXT STEPS
The following steps need to be undertaken:

(a) Work through the Action Plan provided. This sets out a detailed step-by-step plan to ensure compliance. (See end of report)
(b) Review personal data held, how it is stored and the basis for processing it.
(c) Review and refresh existing consents.
(d) Develop Data Privacy Notices.
(e) Review the role of the Data Protection Officer (see also references below).
(f) Review whether Data Protection Impact Assessments are required.

(g) Update data subject access policy.
(h) Update data protection policy.
(i) Review procedures for responding to a security breach and consider security generally.
(j) Start and maintain a log of what data the Council processes.

GLOSSARY AND DESCRIPTION OF ROLES

Consent	Consent is positive, active, unambiguous confirmation of a data subject's agreement to have their data processed for a particular purpose. Consent must be easy to withdraw and must be freely given, provided on an opt-in basis rather than opt-out.
Data Controller	This is the person or organisation (either alone or jointly or in common with other persons) who determines the purpose for which, and the manner in which, any personal data are to be processed. This is the Parish Council.
Data Processor	A processor is responsible for processing personal data on behalf of a controller. The GDPR places specific legal obligations on processors; for example, they are required to maintain records of personal data and processing activities. The processor has legal liability if they are responsible for a breach. This is the Clerk/RFO.
Data Protection Officer (DPO)	The GDPR states that the Data Protection Officer *'should assist the controller or the processor to monitor internal compliance with the Regulation'.* A DPO's duties include: • Informing and advising the Council and its staff of their obligations in the GDPR and other data protection laws. • Monitoring compliance of the Council, both its practices and policies, with the GDPR and other data protection laws. • Raising awareness of data protection law; providing relevant training to staff and councillors. • Carrying out data protection-related audits. • Providing advice to the Council, where requested, in relation to the carrying out of data protection impact assessments (DPIAs) • Acting as a contact point for the Information Commissioner's Office. As noted below, JDH Business Services has quoted for the provision of this service. For this Parish Council, the fee would be £400 per annum for a two-year commitment; thereafter, there would be an annual increment based on CPI. In monitoring compliance, the DPO is not personally responsible where there is an instance of non-compliance, The GDPR makes it clear that it is the controller, not the DPO who is required to '*implement appropriate technical and organisational measures to ensure, and to be able to*

	demonstrate, that processing is performed in accordance with this Regulation.' It is the controller or processor who is required to ''*maintain a record of processing operations under its responsibility*' or '*maintain a record of all categories of processing activities carried out on behalf of a controller'*. The Cheshire Association of Local Councils (ChALC) has informed Clerks that the Government has tabled an amendment to the Data Protection Bill which will exempt all parish and town councils in England from the requirement to appoint a Data Protection Officer, whilst still stating that it is good practice to appoint one.
Data subject	The person about whom personal data is processed. They must be informed about the purpose of processing the data and the legal basis for doing so.
Personal data	Information about a living individual which is capable of identifying that individual; e.g. name, e-mail address or photo.
Privacy notice	A notice from a data controller to a data subject describing how personal data will be used and what rights the data subject has
Processing	Anything done with/to personal data (obtaining, recording, adapting or holding/storing).
Sensitive personal data	This is described in the GDPR as 'special categories of data' and includes the following types of personal data about a data subject. • Racial or ethnic origin • Political opinions • Religious beliefs • Trade union membership • Physical or mental health or condition • Sexual orientation • Genetic data • Biometric data The Parish Council does not hold or process any of this kind of information.

LIST OF KEY AREAS FOR PARISH COUNCILS

The implications are widespread and all local councils will need to have consent, or one of other specific legitimate reasons to hold and process individuals' data.

The following list is not exhaustive but sets out the key areas for local councils and will require a suite of documents to be prepared, the first of which will be a data map to show what information is currently held, the source of the information and with whom it is shared.

(a) Dealing with consent

The Regulation states that an individual, whose information is held, must give their explicit and informed consent for their data to be retained for a set period time, and

processed, which means that the individual must be made aware of how their information is protected, what it is used for, and what the risks are.

There is also a need to consider the position of minors as children under 16 cannot give consent. The Parish Council does not hold any data relating to children.

There are also issues with 'sensitive personal data'. The Parish Council does not hold and has never requested any information which could be described as 'sensitive'.

(b) New privacy policy agreements

The Parish Council does not currently have a Privacy Policy but will need to prepare one which must be user-friendly and written in plain English. The lawful basis for processing data should be explained in the notice.

(c) Individuals' Rights

The following are the rights of 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; This is a new right and allows for the data which an individual provided to the Data Controller, can be provided to the individual in a structured format, to allow it to be provided to another Data Controller.
- The right to object; and
- The right not to be subject to automated decision-making including profiling.

These rights are similar to those in the 1998 Act but have been enhanced.

(d) The right to be forgotten

GDPR allows individuals to withdraw their consent and have their data amended or deleted, known as 'the right to be forgotten'.

(e) Subject access requests

Under the current policy, individuals have the right to request information which is held about them, and the Council is obliged to provide this within 40 days. GDPR reduces this period to a month (it is not clear if this is a calendar month, or 30-31 days).

(f) Pseudonymisation and anonymisation of data

There are some data which cannot be deleted for legitimate reasons; e.g. financial regulatory compliance. In these circumstances, GDPR recommends that the records are 'pseudonymised or anonymised.

(g) Appointing a Data Protection Officer (DPO).

The recommendation is that Councils should check if potential DPOs are cyber security aware and trained. GDPR compliance implies implementing cyber security

regulations and the DPO will need to be up-to-date in respect of cyber security and broader organisational resilience.

JDH Business Services has advised that the latest guidance from the Information Commissioner's Officer (ICO) is that it is unlikely that Clerks/ Responsible Financial Officers can be appointed as the DPO. Therefore, many councils are not going to be able to appoint a DPO internally owing to difficulty in identifying any individual with sufficient independence from data controlling, collection, and processing. A DPO can be an external or internal appointment and, inter alia, must carry out internal audit work to test on-going compliance with GDPR.

JDH has been contacted by several councils requesting a quotation for these services. The company has extensive knowledge of council systems, policies, internal controls and already reports independently to full Council. Therefore, its view is that it can offer this service to councils which are unable to identify an internal resource to carry out this function, or where it is not cost-effective to do so internally.

The Parish Council can consider this matter at the Annual Meeting in May, although the amendment outlined earlier in the report regarding the possible exemption of parish councils from this requirement should be noted.

(h) Data Breaches

The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals.

A report to the ICO is only where a breach is likely to result in a risk to the rights and freedoms of individuals; for example, potential to result in discrimination, damage to reputation, financial loss, loss of confidentiality or other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, those directly affected will need to be notified.

Failure to report a breach could result in a fine, as well as a fine for the breach itself.

SECURITY OF DATA

The Council will need to consider the security of its data.

At present, the Clerk uses his own personal computer on which data is held. Parish Councils need to own a laptop/desktop computer. It is not sufficient for a Clerk to use his/her own equipment for Parish Council work and, at a future meeting, the Council will need to consider purchasing its own laptop, for use by the Clerk.

In practical terms, the laptop would be owned by the Parish Council, but would remain in the Clerk's home. If s/he resigned, the laptop would be given back to the Parish Council for use by its next Clerk. In the meantime, data from the laptop could be stored using cloud technology, accessible by a password. In the event of the Clerk absconding or dying, then the Parish Council has not lost access to its data.

ACTION PLAN (SUMMARY)

1	Raise awareness (amongst councillors, staff and volunteers)
	Decide who will be responsible for the Council's compliance with data protection law.
2	Data audit. Identifying data held, and its source.
3	Identify and document the 'lawful basis' for processing data.
4	Check that processes meet individuals'; new rights.
	Know how to deal with 'subject access requests'.
5	Review how to obtain consent to use personal data.
6	Update policies and notices.
	Privacy Notices – to be prepared.
	Data retention and disposal: Update data retention policy.
	Website: Control access to any restricted area.
	Data sharing: Ensure that personal data is allowed for sharing with others.
	CCTV: Ensure correct signage on display and suitable policy in place.
	Training: Staff to be trained on the basics of personal data security.
7	Build in extra protection for children.
	The Council does not hold any personal data on children and has no reason to collect such data.
8	Update contracts to deal with processing by others.
9	Personal Data Breaches – getting ready to detect, report and investigate.
10	Build data protection into new projects ('Privacy by Design').
11	Appoint a Data Protection Officer.