# General Data Protection Regulation 2016 ('GDPR') and the Data Protection Bill made 'simple' for town and parish councils

First – don't panic. This is about updating a law that is twenty years old. If you comply with the current law you are two thirds of the way to being compliant with the GDPR.

Second – the focus is big organisations processing vast amounts of data or those processing very sensitive data (for example, the NHS or County Councils).

GDPR is an important step in developing a legal framework to reflect the changes in technology since 1995. The Information Commissioner's Office ('ICO') has been heavily involved in drafting the EU regulation. It becomes part of UK law from 25th May 2018. The Data Protection Bill was published on 14th September 2017. The Data Protection Bill and GDPR will complement each other. This note summarises what the changes mean for you.

## 12 steps to GDPR from the ICO (but for parish councils…)

**Awareness** – make sure everyone knows it is happening

**Information you hold** - check what information you hold (and why) and decide whether you do need to keep it.

**Communicating privacy information** – tell people why you are collecting their data, what you will use it for, who you will share it with and how long you will keep it and do this every time you collect data.

**Individuals' rights** – make sure your policy makes clear the rights individuals have (to see their information, correct it, delete it, transfer it)

**Subject Access Requests** – make sure your policy is easily available and easy to understand

**Lawful basis for processing data** – are you processing by consent?

**Consent** – pre-ticked boxes (or apathy) are no longer enough. You need **explicit, informed** consent.

**Children** – verification of age and seeking parental consent, if necessary. Thirteen will probably be UK 'age of consent' (that is children thirteen and over are generally deemed able to consent to the processing of their own personal data).

**Data breaches** – ensure you have a process for identifying breaches and reporting them.

**Data Protection by Design and Data Impact Assessments** – systems and policies should have safeguards for personal data built in. Ask questions about any IT systems (or equipment) you are buying

**Data Protection Officer** – formally nominate someone to carry out this role and ensure the council is aware what the job entails.

**International** – you probably don't think this applies but remember 'cloud services' are not fluffy, benign clouds they are large data warehouses somewhere abroad – that makes transferring data there an international transfer. Look at the contract provisions of your service provider

## Six Data Protection Principles

## (reduced from the current eight)

1. **Lawfulness, fairness and transparency**

2. **Purpose limitation** – collected for specified, explicit and legitimate purposes – set this out clearly in your **Privacy Notice**. Tell people why you need their data when you collect it from them. Tell them what you will do with it, who you will share it with and how long you will keep it. Don't just do this once. Tell them whenever you collect data.

3. **Data minimisation** - adequate, relevant and limited to what is necessary.

4. **Accuracy** – up to date and accurate. Delete, or correct, without delay if inaccurate.

5. **Storage limitation** – don't keep longer than is necessary or legally required.

6. **Integrity and confidentiality** – keep data both physically and electronically secure.

## Six legal purposes for the lawful processing of data

## (see principle one above)

**Consent** – this is the usual basis for processing but the burden of proof is higher under GDPR.

Consent means 'freely given specific and informed indication of wishes by which data subject signifies agreement to their personal data being processed'

Consent is **not** freely given if there is no real choice or refusal or withdrawing consent will cause detriment. Withdrawing consent should be as easy as giving consent. The burden of proof is on the data controller to prove consent given. Consents should be regularly reviewed and updated (ICO recommends every two years).

**Performance of contract.** This means you have to collect and process the data to provide the service

**Compliance with legal obligation**

**Vital interests of data subject** e.g. monitoring epidemics, humanitarian emergencies

**Public interest** e.g. use of personal data for collection of income tax

**Legitimate interests of data controller** e.g. for prevention of fraud

## Greater accountability for local councils

## How to comply

- Have an appropriate data protection policy
- Appoint a Data Protection Officer
- Ensure all staff and councillors have Data Protection training
- Carry out a Data Protection Audit (work out what information you are holding, where, why and for how long)
- Think about Data Protection when implementing decisions (this is called a 'Data Protection impact assessment')

- Think about ensuring your systems have Data Protection built in. This means 'privacy by design' and 'privacy by default' but what does **'privacy by design'** and **'privacy by default'** actually mean? It means building in security of data to the systems and processes you use rather than relying on people to remember.
- Personal data should not be made available to an indefinite number of people so 'we will only share your personal data with carefully selected third parties' (sound familiar?) is no longer acceptable.

## Enhanced rights for all individuals

All individuals who have dealings with the council, including you, have these rights and the council needs to take account of these rights

**Requests for information** (**'Subject Access Requests'**)

Under the GDPR a data controller may not charge for dealing with a request for access to personal data (a 'subject access request'). You must respond promptly and, in any event, **within one month** (for complex, or numerous, requests this period can be extended by a further two months). There is a discretion to charge a reasonable fee, or refuse to comply if the request is unfounded, or excessive, but the data controller bears the burden of proving the request was unfounded or excessive. Third parties can ask for information but must still prove they have consent, or justify why it is appropriate, as they do now.

**Note - you will no longer be able to charge the £10 fee but it does make the timescales (and the approach to dealing with vexatious requests) similar to Freedom of Information and Environmental Information Regulations requests.**

**Transparency**

People should know whether they are obliged to provide their personal data and what the potential consequences are. This needs to be clear at the point of collecting the data.

**Rectification**

The right to have inaccurate personal data corrected. If inaccurate data has been shared there is an obligation to inform any recipients of the correction unless this is impossible or would involve a disproportionate effort.

**Erasure ('the right to be forgotten')**

This is **not** an absolute right. It does not apply if there is a lawful reason for continued processing. This might be a factor, for example, where you have employment records and someone requests that details of a grievance, or a disciplinary, be removed.

**Restriction of processing**

Where there is a dispute about the processing of the data then affected personal data may only be processed with the data subject's consent, for establishing or defending legal claims, for the protection of another natural or legal person's rights or for reasons of important public interest. This restriction continues until the dispute is resolved.

**Data portability**

This allows a data subject to instruct a data controller to transmit their personal data to another controller where it is technically feasible to do so (useful if you want to change banks

or energy suppliers). Interoperable formats enabling portability are encouraged but there is no obligation to maintain, or adopt, technically compatible systems.

**Objection to processing**

A data subject can object to processing of their data and a data controller must respond within one month (with a potential two month extension for complex, or numerous, requests). Processing includes profiling for the public interest, for direct marketing and for historical research or statistical purposes. Other than direct marketing the request is subject to the application of the public interest test.

**Automated decision making**

This is a decision made by technology alone. This includes 'profiling' for evaluation of an individual's health, reliability, location or economic situation. The data subject must be given the right to human intervention and to contest the automated decision. This is probably not an issue for parish councils yet.

## Data Protection Principle Six

## Integrity and confidentiality – keeping personal data secure

Keeping data secure means keeping IT systems secure. That means strong passwords, regular backups, keeping software updated and applying patches as soon as possible. It means encryption, anonymising data and having guidance for the storage of council business on personal tablets or phones. ***It means having council email addresses.***

## Mandatory data breach notification

You have 72 hours to notify the ICO of a data breach if it is serious. If the breach poses a high risk to data subjects they must be notified 'without undue delay'. High risk means financial loss, damage to reputation or discrimination. The ICO is developing a new phone reporting service and web reporting form to ensure there is access to immediate advice to help when a data breach happens.

## Immediate impact of GDPR and a 'to do' list

1. Notification is abolished (this is the annual registration with the ICO to 'notify' the ICO that you process personal data). Continue to maintain the record of processing you already have (and keep it updated) but you will no longer need to send off the annual form or pay a fee to the Information Commissioner's Office (ICO) from 25th May 2018.

2. Appoint a Data Protection Officer. The person must have
    - appropriate expertise;
    - be able to report to the highest level in the organisation, that is, to the Clerk and/or Full Council (as appropriate);
    - be able to operate independently and
    - cannot be dismissed for carrying out their role properly.

In smaller organisations the tasks will be:

- dealing with subject access requests and 'right to be forgotten' requests;
- reporting data breaches to ICO and affected data subjects;
- implementing and updating policies and procedures;
- dealing with enquiries and complaints from data subjects.

3. Review your policies on data security, retention and responding to requests for information because they should all work together. This includes a clear process (that everyone is aware of) for identifying a breach of data security and deciding whether it needs to be reported to the ICO.

4. Put in place a Privacy Notice [see attached generic Privacy Notice] and ensure you have appropriate privacy wording whenever you collect personal data

5. Check your IT security – do you back up regularly? Are you applying updates as soon as available? Patches are issued to deal with known holes in security – those patches must be applied. ***It means having council email addresses.***

6. Check you are obtaining **explicit consent** to use personal data and not relying on implied consent, pre-ticked boxes or inactivity (apathy). The ICO have a privacy notice checklist which is included in this package and can be found on their website at www.ico.org.uk.

7. When considering using cloud services look for the Cloud Infrastructure Service Providers in Europe (CISPE) Code of Conduct which provides for:
    - An effective, easily accessed framework for complying with the EU's GDPR
    - Excludes the re-use of customer data
    - Enables data storage and processing exclusively within the EU
    - Identifies cloud infrastructure services suitable for different types of data processing
    - Helps citizens to retain control of their personal and sensitive data

For further information (and new guidance when available) please refer to the 'Data Protection Bill' and 'Getting Ready for the GDPR' sections of the ICO website which are regularly updated.

 September 2017

## Glossary

**Data controller** means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

**Data processor**, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

**Data subject** means an individual who is the subject of personal data

**Personal data** means data which relate to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

**Sensitive personal data** means personal data consisting of information as to -

(a) the racial or ethnic origin of the data subject,

(b) their political opinions,

(c) their religious beliefs or other beliefs of a similar nature,

(d) whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) their physical or mental health or condition,

(f) their sexual life,

(g) the commission or alleged commission by them of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings

**Processing**, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data.