# 38 DATA PROTECTION

The current Data Protection Act 1998 becomes stricter on 25 May 2018 under the General Data Protection Regulations (GDPR). They will introduce more transparency and greater protection of personal data – as well as much larger fines for non-compliance. They will apply to all organisations - there are no exemptions for parish/town councils.

**Data Protection Principles:**

**1 Personal data must be processed fairly and legally**

RTC will have to make it clear why it is collecting data and what it intends to do with it.

Example of a notice that could be displayed on a web site:

***How the information you provide will be used***

*General Data Protection Regulations: Any personal information such as name, postal address, telephone number and email address given via this web site will be used to provide a requested service only and will not be disclosed to any third party without your prior permission, or unless we are required to do so by law.*

**2 Personal data must be obtained only for specified and legal purposes – and must be processed only in a way that is consistent with the specified purpose.**

**3 Personal data must be adequate, relevant and not excessive for the purpose it is processed for.**

**4 Personal data must be accurate and, where necessary, kept up to date.**

**5 Personal data processed for any purpose must not be kept longer than is necessary to fulfil that purpose.**

**6 Personal data must be processed in line with the data subject's rights.**

**Other considerations:**

Appropriate security measures must be taken to protect against unauthorised or illegal processing.

Transferring personal data outside of the European Economic Area is restricted unless the rights and freedom of data subjects are protected.

**Data Protection Assurance**

Required: Policies

Training

Registration (with the Information Commissioner's Office)

Processes to evaluate new projects

**Data Sharing and Subject Access**

Required: Policies

Training

Transparency

**Direct Marketing**

Required: Consent

**Information Security**

Required: IT security

Training and induction

Portable equipment/removable media safeguards

**Data Protection Officer (DPO)**

A DPO must be appointed. The Department for Digital, Culture, Media & Sport (DCMS) has advised NALC that:

> *it is a matter for each public authority to determine who should act as the DPO and what level of knowledge and expertise they require . . . In order to avoid a conflict of interest a DPO should not determine the purpose or manner of processing personal data. Provided that a parish council is satisfied that a clerk does not do this then they could act as the DPO . . . We also believe that an alternative is to appoint someone external to the council. Various options exist including sharing a person between parish councils or sharing with the district council or other principal local authority.*

**Data Controller**

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 Control**

Parish councils are data controllers because they collect and use personal data. Examples include information about:

Current, former and prospective members of staff

Local residents

Suppliers and service providers

Enquirers

Complainants

Individuals captured on CCTV images

Councillors (when acting in an official capacity)

Relevant parish council activities include:

Maintaining/Managing accounts and records

Recruiting/Managing staff

Promotion/Provision of council services

Making contracts for the supply of goods and services

Managing premises

Administering grants

Crime prevention via CCTV

Corporate/Office administration

Resident surveys

**Privacy (Fair Processing) Notices**

These are a reference to particular set of information which a data controller is required to provide to an individual (the 'data subject') when it is processing his/her personal data. The use of Privacy Notices implements the first Data Protection Principle.

The content of a Privacy Notice depends on whether or not the personal data has been collected directly from the data subject.

At the time personal data is obtained directly, the data controller must provide the data subject with:

The identity and contact details of the data controller

The contact details of the DPO

The purpose of the data processing

The recipients (or categories of recipients) of the personal data

The period for which the personal data will be stored

The existence of the right to request access to the data or object to its processing

The right to withdraw consent to store/process data

The right to lodge a complaint with the Information Commissioner

The existence of any automated decision making

Where a data controller wants to process personal data for a purpose other than that for which it was collected originally the controller must provide the data subject with this information in advance.

Privacy Notices may be provided orally, in writing, via signage or electronically.

**Subject Access Requests (individuals requesting to see what information is held about them)**

Individuals have the right to:

Confirmation that their data is being processed

Access to their personal data

The purpose/s of the data processing

The categories of the personal data

To whom the personal data have been – or will be – disclosed

The period for which the data will be stored (or when it will be destroyed)

The existence of the right to request rectification/erasure of data

The right to lodge a complaint with the ICO

(Where the data has not been collected directly from the data subject) The source of the data

The existence of any automated decision making

Where a subject access request is made electronically, where possible, the information should be provided electronically. Howsoever it is provided, information must be provided in an accessible and clear form.

(Unless 'manifestly unfounded or excessive') Information must be given free of charge.

A 'reasonable fee' may be charged to supply further copies of the same information

Information must be provided within one month of receipt of the request. This may be extended to 3 months if the information requested is complex or numerous.

The data controller may use reasonable means to verify the identity of the person making the request.

**Preparation required for 2018 (TH and HC)**

Data audit and cleansing (destroying unnecessary data)

Training and induction

Drafting privacy (Fair Processing) Notices

Drafting policies and processes

**Support**

NALC has produced a number of briefing notes and SSALC has arranged briefings for clerks.

DCMS has undertaken to *find a way to ensure that generic ICO guidance (pending) can filter into more specific content to assist parish councils* and to *Engage with the Local Government Association (LGA) to see how their members may be able to assist with sharing DPOs.*