Hirwaun & Penderyn Community Council

Data Protection and the Council and Councillors

Significant new obligations are being demanded from Councillors.

The amended data Protection Legislation ("the Legislation") and advices and guides from the Information Commission Office (ICO) www.ico.org.uk. set out how Councils/Councillors must deal with personal data/information (personal data) from 25 May 2018.

What personal data is included and protected by the Legislation?

The Legislation applies to 'personal data', which means any information relating to "an identifiable person who can be directly or indirectly identified by reference to an identifier" (the individual(s)). A fuller definition is set out in Appendix 1.

A good starting point is to assume that if you have personal data you are subject to the Legislation. However, there is an exception found in the ICO guide to elections if the Councillor only holds paper records (see below).

The definition includes a wide range of personal identifiers to constitute personal data, including name, identification number, location personal data or online identifier reflecting changes in technology and the way organisations collect information about people.

Both automated personal data and manual filing systems are included in the Legislation where personal data is accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

The Legislation requires "good information" handling by the Council and the Councillor.

What is "good information" handling?

The Legislation is based around eight principles of "good information" handling. These give the individuals specific rights in relation to their personal information and place certain obligations on Councils/Councillors. The eight principles are set out in Appendix 2. These give individuals specific rights in relation to their personal data and place specific obligations on the Council when processing it. The Legislation places the individual in charge.

How does the Legislation relate to the Council and the Councillors?

The Personal Data Protection Bill (which will be enacted before 25th May) is highly likely to define public authorities as at present but will add to existing obligations. Town and Community Councils therefore will continue to be included in the definition and as presently the Council will be a "personal data controller".

The Council being a data controller does and will determines “the purposes and means” of processing personal data. Even if not presently registered, the Council will need to be registered as a personal data controller because it holds personal data- from 25 May the fee is likely to be £40. There are substantial fines for breaches of the Legislation.

As it is a personal data controller, the Legislation also requires that there is in place a “personal data processor” appointed by the Council. The personal data processor is likely to be the Council clerk/chief executive and will be responsible to implement the “purposes”, “the means” and “to process” the personal data policies- an agreement will need to be in place to that effect.

How does the Legislation involve and affect Councillors?

Normally Councillors are considered to have three different roles:

- as members of the Council;

-as representatives of individuals such as when dealing with complaints; or

-when they may represent a political party, particularly at election time.

When using personal information Councillors should consider the context in which that information was collected to decide whether their use of the information will be fair and lawful as required by the Legislation.

As members of the Council

Councillors may have access to, and process, personal data similarly to employees. In this instance it is the Council rather than the Councillor that determines what personal data is used for and how it is processed. For example, if a member of a committee has access to personal data files in order to decide whether the Council should undertake action, the Councillors are carrying out the Council’s functions and so do not need to register in their own right.

As representatives of individuals

When Councillors represent individuals, they are likely to have to register in their own right. For example, if they use personal information to timetable “surgery” appointments or take forward complaints made by local residents.

However, where a Councillor is representing an individual, who has made a complaint, the Councillor in consequence will usually have the implied consent of the resident/individual to retain the relevant personal data provided and to disclose it as appropriate. The individual will also expect that the Council (or organisation) the subject of the complaint will disclose personal data to the Councillor. If there is any uncertainty regarding the resident’s wishes, it would be appropriate to make direct contact with the individual to confirm the position.

Note:

-Sensitive personal information (see Appendix 1) is treated differently; for example, where consent is being relied on, this should be explicit in nature. However, in the context of a complaint, Councillors – and organisations making disclosures to them - will usually be able to rely on the Personal Data Protection (Processing of Sensitive Personal data) (Elected Representatives) Order 2002 as a condition for processing.

Political purposes/Elections

When acting on behalf of a political party, for instance as an office holder, a Councillors is entitled to rely upon the registration made by "the party".

When candidates campaign on behalf of political parties to be a Councillor, they can rely on the parties' registration if the party determines how and why the personal information is processed for the purpose of their individual campaigns.

Similarly, candidates can use personal information, such as mailing lists, legitimately held by their parties. However, personal data they hold in their role as representative of residents, such as complaints or on file should not be used without the consent of the individual.

When campaigning for election to an office in a political party, Councillors should only use personal information controlled by the party if its rules allow this. It would be wrong, for instance, to use personal data which the candidate might have in their capacity as the local membership secretary, unless the party itself has sanctioned.

If a prospective Councillor is not part of any political party but campaigning to be an independent Councillor for a ward, there will be a need to have registration with ICO.

Note:

-Personal information held by the Council should not be used for political purposes unless both the Council and the individuals concerned agree. It would not, for example, be possible to use a list of the users of a particular service for electioneering purposes without their consent. An example would be using a Council list of library/community hall/museum users to canvass for re-election claiming say a Councillor or candidate had previously opposed the closure of local libraries.

-Candidates for election should be aware that political campaigning falls within the definition of direct marketing. Consequently, they should have regard to the requirements of the legislation which set out specific rules that must be complied with for each type of marketing communication.

For further information on elections, the Information Commissioner has produced "Guidance on Political Campaigning".

Multi-member wards.

When Councillors are elected under a multi-member system where more than one Councillor represents a ward there may be situations where a Councillor who represents an individual may need to pass on that particular individual's personal information to another Councillor in the same ward. The Councillor will only be allowed to disclose to the other ward Councillor the necessary personal data, for example, to deal with the individual's(s) concerns, where the particular issue raises a matter which concerns other elected members in the same ward, or where the individual has been made aware that this is going to take place and why it is necessary.

If an individual(s) objects to a use or disclosure of the information, the objection should normally be honoured.

Should a Councillor pass on personal information which is not connected to the resident's case?

Where a Councillor wishes to share an individual's complaint with another Councillor(s) because it is an issue of general concern, the Councillor should let the resident know of the intent to provide the details of the complaint to the other ward Councillor rather than give a general description of the complaint to the other ward Councillor.

If the resident objects, then the wish is to be respected and only the general nature of the complaint is shared.

Payment of a personal data protection fee/registration?

When considering whether a Councillor needs to register the processing with the Commissioner, Councillors must first decide in which role they are processing personal information (see above).

It might well be that registration and payment of a fee is required and the ICO has a form for registration by Councillors to simplify the registration.

Note:

-RCTCBC Councillors are registered under the present legislation,

-According to paragraph 11 of the ICO "Advice for Elected and Prospective Councillors" an exemption from registration exists where the only personal information which is processed takes the form of paper records.

What Security arrangements should be used?

A Councillor should arrange appropriate security to protect personal data and must consider the nature of the personal data and the "harm" and consequences for the individual that could result. ICO advises that Councillors "consider technical and organisational measures, such as the use of passwords, computer access privileges, procedures and training" to keep the personal data safe. Councils should also take appropriate measures in the same way and provide training.

Offences

The Legislation contains a number of criminal offences not only for Councils but also for Councillors for breaches of the Legislation, including:

-Failure to register when required to do so. For example, Councillors who hold computerised records of individuals' details for casework purposes would commit an offence if they had not registered this use of personal data;

-Making unauthorised disclosures of personal data. For example, a Councillor who discloses personal information held by the Council to the "party" for electioneering purposes without the Council's consent;

-Procuring unauthorised disclosures of personal data. For example, a Councillor who obtains a copy of personal data for Council purposes allegedly, but in reality for the Councillor's own personal use (or the use of a political party), is likely to have committed an offence.

Does the Council need to appoint a Personal Data Protection Officer?

Attached at Appendix 3 is guidance on this topic extracted from the ICO advice "General Personal Data Protection Regulation (GDPR) FAQs for small local authorities". Advice has also been provided by OneVoice Wales and SLCC (Society of Local Council Clerks).

Additional information

Further information and detail can be obtained from the ICO at www.ico.org.uk.

Appendix1-Personal Personal data

-Personal data

“The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location personal data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

-Sensitive personal data

The GDPR refers to sensitive personal data as “special categories of personal data”.

The special categories specifically include genetic personal data, and biometric personal data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).”

Note:

GDPR is the General Data Protection Regulation.

Appendix 2-the Eight Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

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

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of personal data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of personal data subjects in relation to the processing of personal data.

Appendix 3-ICO Guidance Data Protection Officer

"I work for a small local council, do I need to appoint a personal data protection officer (DPO)?

Yes. Under the GDPR, you **must** appoint a DPO if you:

- are a public authority (except for courts acting in their judicial capacity);
- Your core activities include large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- Your core activities include large scale processing of special categories of personal data or personal data relating to criminal convictions and offences.
- There's a section on DPOs and when they need to be appointed in our Guide to the GDPR.

Can organisations share a DPO?

You may appoint a single personal data protection officer to act for a group of public authorities or bodies, taking into account their organisational structure and size. There is more on appointing a DPO in our section on DPOs and when they need to be appointed in our Guide to the GDPR.

Can the DPO be an existing employee?

The person you appoint as a DPO can be an existing employee, provided the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interest.

What is a conflict of interest in relation to a DPO?

Conflict of interest means a conflict with possible other tasks and duties. This means the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. More information on this can be found at questions 9 and 10 of the Article 29 DPO FAQ's and in the Article 29 guidelines on DPO's

What are the legal implications for a DPO?

DPO's are not personally responsible for non-compliance with the GDPR. The GDPR makes it clear that it is the controller or the processor who must demonstrate that processing is undertaken in compliance with the GDPR. Personal data protection compliance is the responsibility of the controller or processor."