Briefing for Councillors on Data Protection

Questions and Answers

This briefing is about the introduction of the new data protection law, which is called the General Data Protection Regulation 2016 and is known as GDPR. The government also introduced the Data Protection Act 2018 (DPA) which amended the GDPR.

The data protection laws provide a legal framework for the processing of personal data, the rights of individuals and enforcement powers of the Information Commissioner's Office.

Both data protection laws started on Friday 25th May 2018.

Explaining the jargon:

- Personal data is information about a living person, which is capable of identifying the individual.

- Processing is anything done with or to personal data, including collecting, using, storing and deleting it.

- The 'data subject 'is the person about whom personal data is processed e.g. a resident.

- The 'data controller' is the person or organisation who determines the how and what of data processing.

- The Information Commissioner's Office (ICO) is responsible for the supervision of GDPR and can issue enforcement notices and fines. Their website is www.ico.org.uk.

1. Introduction

Councillors are likely to have three different roles:

- They represent residents of their ward, for example, in dealing with complaints.

- They act as a member of the Council, for example, as a cabinet member or member of a committee; and

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

Depending on the role the Councillor has at the time, the Council may be able to disclose personal information to them. In doing so, it will often be

necessary to restrict the use of any personal information provided for specific purposes.

Councillors may also obtain personal information from residents.

2. How does GDPR affect Councillors?

Elected members are data controllers under GDPR and are responsible for the personal data that they collect, store, use and delete.

3. New data protection law (GDPR)

The new data protection law replaces the Data Protection Act 1998. It places more emphasis on transparency, openness and the information that you will need to show that you are complying with the law (the idea of accountability).

4. What is personal data?

Any information relating to an identifiable person who can be directly or indirectly identified.

The definition provides for a wide range of identifiers and includes: name, date of birth, identification number (e.g. account or reference number), location data, online identifier (e.g. online information and email address).

5. What is special category data (sensitive personal data)?

Special category personal data includes: race, ethnic origin, political opinion, beliefs, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.

Usually, informed and written consent is required to process this type of data. However, Councillors can process special category data under the new Data Protection Act 2018 exemption without informed and written consent.

This category of data must be protected at all times because of its sensitivity and extra care must be taken. If the communication from a resident is unclear, which may include sensitive personal data, you should seek clarification.

6. How do I comply?

The GDPR requires that personal data shall be:

- Processed lawfully and not further processed in a manner that is incompatible with those purposes (explained further below).

- Collected for specified, explicit and legitimate purposes (e.g. an enquiry from a resident about a Council matter).

- Adequate, relevant and limited to what is necessary to the purposes for which they are used.

- Accurate and kept up to date.

- Kept for the minimum period necessary and with justification, and

- Held securely.

7. How do I show that I am processing personal data lawfully?

You need a lawful basis for receiving, storing and using personal data.

The two likely lawful bases that you will use are:

- Consent (freely given and this must be recorded and managed). Keeping a record of the communication and action(s) taken.

- Public task or official authority (e.g. supporting or promoting democratic engagement including casework).

8. What are the rights of the data subject (living person)?

Individuals have rights and these include:

- The right to be informed how their data is processed (the use of privacy notices to inform residents).

- The right to access (an individual's request for personal data that you hold about them).

- The right to rectification (correction of data you hold).

- The right to erasure (also known as the right to be forgotten). This does not mean that a person can immediately request that his or her personal data is deleted.

- The right to restrict processing (stop using their personal data).

- The right to portability will only apply in some circumstances e.g. when consent is used, and

- The right to object in some circumstances about the use of their personal data.

9. Do I need consent for existing records held?

No; you should review and consider whether you still need it for the purposes it was given to you.

10. Do I need to delete information held on a mailing list?

No; if consent was already given for them to be on the mailing list.

11. Do I need consent to name my constituent when engaging the Council, government on their behalf?

No; but you will need to be clear with them what will happen to their information and how you will use it. In some cases, you may need to go back to the resident if there is uncertainty over the resident's wishes.

12. How do I keep information safe and secure?

It is very important that personal data that you collect, hold and use is protected and you may have to provide information about how this information is kept safe and secure by the Information Commissioner's Office.

- Only use the email account provided by the Council for communication with residents and officers. **Your personal email address must not be used!** The Council's computers and network are secure and we have implemented security controls to protect the information held and used by Councillors and employees. We can provide evidence if required by the ICO or individuals who are concerned about the security of their personal data and give re-assurance.

- Before sending an email check that it is going to the right person. Email addresses look the same or is held by the computer for ease of use. Always check!

- Never forward an email to another person without checking the information or attachment(s) because you may accidently disclose too much information or information that should not have been disclosed. If in doubt create a new email with only the information that you want to share.

- When sending an email to a group of people outside the council enter the email addresses in 'BCC' and don't use 'To', unless the individuals know each other's email address. An email address is personal data and the use of BCC will hide the email addresses used.

- Be careful of the environment that you are working in when using personal data because you may be overheard or information seen on your computer or iPad.

- Password(s) and security code(s) issued must be protected and not shared, disclosed or attached to devices.

- Make sure that your computer, laptop, iPad or smartphone is locked when not in use to protect the information and to stop unauthorised access to the device.

- Personal data is confidential and is protected by GDPR. Never share information with family or friends or allow access to personal data disclosed to you in your role as a Councillor.

- You should avoid printing and carrying papers with personal and sensitive data because it is not protected, can easily be lost or stolen, may not be backed-up or is the only document held.

13. What is a data breach?

A register of data breaches must be maintained by Councillors and serious breaches reported to the ICO within 72 hours. Examples are where personal data is lost (e.g. papers are left on a train), stolen, hacked (e.g. if an ICT device is lost or there is evidence that your laptop has been hacked) or email sent by you to the wrong person.

If there is a data breach, please inform the Data Protection Officer, Ian Gibbs, immediately at ian.gibbs@onesource.co.uk, who will provide advice and support. It is important that steps are taken to rectify the breach as soon as possible and advice will be provided to assist you.

14. What are the possible consequences of a breach?

Where personal data incorrectly enters the public domain as a result of a data breach it can cause significant harm to those individuals and to their families and others. That harm may include psychological, emotion or financial harm. Data breaches are also likely to cause reputational damage to those responsible for the breach. Fines for breaches have always been part of the Data Protection regime but under the new legislation those fines are significantly higher.

15. Do I need to inform the Information Commissioner's Office that I am a data controller?

Elected Members must register as a data controller under the data protection law and we do it for you.

16. Do you need a privacy notice?

Yes, and we have done this for you. It is on the Council's website on the data protection webpage. You must inform residents how their personal data is collected, stored, used, deleted and protected.

17. When can the Council disclose personal data to Councillors?

A local authority does not generally have to get the express consent of an individual to disclose their personal information to an elected member, as long as:

- The elected member represents the ward in which the individual lives.

- The elected member makes it clear that they are representing the individual in any request for their personal information to the Council.

- The information is necessary to respond to the individual's complaint

Further information

For further information, advice and support please contact Ian Gibbs, the designated Data Protection Officer, ian.gibbs@onesource.co.uk.

Ian Gibbs,
Head of ICT Governance and Security (Data Protection Officer)
01.06.2018