The General Data Protection Regulation (GDPR) Guidance for members

What is the GDPR?

The law on Data Protection has changed from 25th May 2018. The General Data Protection Regulation (GDPR) is a new, Europe-wide law that replaces the Data Protection Act 1998 in the UK and supersedes the **UK Data Protection Act** 1998 (DPA 1998). It is part of the wider package of reform to the data protection landscape that includes the Data Protection Act 2018 (DPA 2018).

The GDPR sets out requirements for how organisations need to handle personal data from 25 May 2018. In addition to other changes, it will enhance the rights of people whose data is held (known as data subjects in the Data Protection Act) and give them more control over what happens to their data.

It also allows for financial penalties to be imposed on any organisation that breaches those rights or does not comply with the 'accountability principle' – which basically means that data controllers and data processors i.e. organisations and certain individuals – including councils, need to put technical and organisational measures in place to protect the data they hold from loss, unauthorised access etc and to ensure the rights of data subjects are protected.

The GDPR has direct effect across all EU member states and has already been passed. This means organisations will still have to comply with this regulation and we will still have to look to the GDPR for most legal obligations. However, the GDPR gives member states limited opportunities to make provisions for how it applies in their country. One element of the Data Protection Act 2018 is the details of these. It is therefore important the GDPR and the 2018 Act are read side by side.

What else does the DPA 2018 Act cover?

- The DPA 2018 has a part dealing with processing that does not fall within EU law, for example, where it is related to immigration. It applies GDPR standards but it has been amended to adjust those that would not work in the national context.
- It also has a part that implements the EU's Law Enforcement Directive. This is part of the EU's data protection reform framework and is separate from the GDPR. The Bill has provisions covering those involved in law enforcement processing. The ICO has produced a 12 step guide for preparing for the law enforcement requirements (part 3) of the DP Bill. Our webinar also has helpful guidance on the preparations organisations should be making to prepare for the change in legislation.
- National security is also outside the scope of EU law. The Government has decided that it is important the intelligence services are required to comply with internationally recognised data protection standards, so there are provisions based on Council of Europe Data Protection Convention 108 that apply to them.

- There are also separate parts to cover the ICO and our duties, functions and powers plus the enforcement provisions. The DPA 1998 is being repealed so it makes the changes necessary to deal with the interaction between FOIA/EIR and the DPA
- The new regime is more stringent and gives the data subject enhanced rights.
- In the new regime, the eight principles become six principles

The 6 GDPR Data Principles

The six general principles under the new legislation are very similar to the current law:

1. Personal information shall be processed lawfully, fairly and in a transparent manner.
2. Personal information shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Personal information shall be adequate, relevant, and limited to what is necessary
4. Personal information shall be accurate and, where necessary, kept up-to-date
5. Personal information shall be retained only for as long as necessary.
6. Personal information shall be processed in an appropriate manner to maintain security.

You must have a lawful basis to process personal data. Consent is one of them but there are alternatives. There are six available lawful bases set out in Article 6 of the GDPR. These are consent, contract, legal obligation, vital interests, public task, legitimate interests in total. No single basis is better or more important than the others. Which is most appropriate will depend on your purpose and the relationship with the individual.

What information does the GDPR apply to?

The GDPR applies to 'personal data', which means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. You can find more detail in the key definitions section of the ICO's Guide to the GDPR by following this link https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/.

Personal Data (PD) includes:

- an identifier, e.g. a name, email address, phone number
- personal identification numbers, e.g. bank account, national insurance number

- factors specific to an individual's physical, physiological, genetic, mental, economic, cultural or social identity. This would include anything about a disability.

New kinds of identifying information which GDPR includes in the definition of personal data are:

- location data - data that has any kind of geographic position attached to it, e.g. data collected by wireless networks, swipe cards and smart mobile devices that provide location tracking
- online identifiers, e.g. mobile device IDs, browser cookies, IP addresses

Special Categories of Data (set out in Article 9 of GDPR) are those which are more sensitive relating to, race, ethnicity, political opinion, genetic or health related data and sexual orientation, and so needs more protection.

If you are processing data that falls within this category, you must first identify a lawful basis under Article 6 and a separate condition for processing special category data under Article 9.

The broadening in the definition of personal data is important because it reflects changes in technology and the way that organisations collect data about individuals.

Under the Data Protection Act 1998 it has been a requirement for you as a councillor to be registered as a Data Controller with the Information Commissioners Office (ICO) and pay a fee. (Some Councils have paid the fees for their Councillors).

This is because as a councillor

1. You make use of personal data provided by your council in the same way as an officer of the council might make use of data. Council officers and its suppliers will be subject to the controls of GDPR in the same way they are under DPA 1998. You will be covered by your Councils notification and fee.
2. You use personal case work material in your own right when you collect or are given personal data through communications with your residents.
3. You access, collect and deploy personal data through your political campaigning and activation – with or without the use of political agents or political parties if you represent one.

As a Data Controller you will need to comply with the new GDPR and Data Protection Act 2018 unless as a Councillor you do not make any use whatsoever of a computer/tablet/smart phone etc in connection with your Councillor activities of any sort.

You should already be keeping personal data secure and only using your official email address to respond. You will already be aware to be careful with whom you share personal data and to keep information for no longer than you need to. This might include other councillors in multi member wards. The new GDPR/ACT will

place a duty on you to keep certain records as it is your duty to show that you are complying with the law. It is also designed to give data subjects (your residents) greater rights to control and access the data you hold about them.

New requirements:

- Keep a record of your processing activities, this is to show your compliance with the legislation.
- Give a more detailed Privacy Notice when you collect personal data.
- Tell subjects of their rights.
- Have appropriate security measures in place to protect personal data you hold.
- Regularly review and delete 'old' data you no longer need.
- Report any breaches to the ICO within 72 hours.

Record Keeping

To comply with the Act, you must keep certain records if your processing is more than occasional e.g. for complaints, or you are processing 'special categories of data' e.g. anything concerning race, religion, health, sexual orientation etc. It is possible that you will have health data concerning your residents and you should record (perhaps in a word document):

(i) The name and contact details of the Data Controller – yourself;
(ii) The purpose of your processing and legal basis for it e.g. to investigate complaints;
(iii) The categories of data you hold and the categories of data subjects' e.g. name and address, email, medical information for constituents and complainants;
(iv) Anyone you share the data with e.g. other Councillors/Council Officers/other services.
(v) How long you keep data for e.g. 6 months after the case is closed
(vi) What security you have in place to protect it e.g. password protection, only using secure council provided email address, documents locking in a cupboard etc.

The information Commissioner can ask to see this record to ensure your compliance.

Privacy Notices

You are required to give a Privacy Notice to the person you collect personal data from at the time you collect it.

This could be a standard paragraph at the end of an email when you acknowledge receipt of a complaint or you can give it verbally if you take a telephone call in which case you should record that you have given it verbally.

You should not use personal data other than for the purpose which you stated when you collected it. If you wish to use it for another purpose then you should return to the person and seek their consent for this additional processing. If you are collecting special categories of data then the person should give you explicit consent to process this data. This might mean you should obtain their signature and you should keep a record that they have given consent.

The GDPR sets out the information you should supply and when individuals should be informed.

A Privacy Notice should include:

(i) That you are the Data Controller and your contact details;
(ii) The purpose of processing and legal basis for doing so (to assist with their complaint);
(iii) Who you will share it with e.g. other Councillors/Council Officers/ any other agencies;
(iv) The retention period i.e. how long you will keep it for e.g. for 6 months after their complaint has been finalised;
(v) That they can withdraw their consent to you processing their data by contacting you and asking you to stop doing so;
(vi) That they can access a copy of the information you hold, ask for it to be corrected if it is wrong or for it to be deleted;
(vii) To contact you if they have a complaint about how their data is handled and if it is not resolved to contact the ICO.

There's more information in the ICO's right to be informed section of the Guide to the GDPR. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

Rights

As stated in the Privacy Notice you must comply with certain rights which the data subjects have. This includes allowing them to access all the data you hold on them, this is usually by way of a copy of emails or letters. You have one month to comply with a request which is called 'subject access'. You must remember NOT to supply them with anyone else's personal data as they are only entitled to access their own.

They can also ask for their data to be corrected, moved, restricted or erased in certain circumstances.

Security

You should ensure the security of the personal data that you hold by only using your official email address and being careful if you work in public areas so that you are not overlooked. You should not leave documents or computers/iPads on whilst you are out of the room and should ensure that you have a password to access the necessary files. You should ensure the device that you use is stored securely when

not in use. When emailing you should put the minimum amount of personal data necessary in order to make sense and avoid references to other identifiable people where possible.

You can find more guidance in the security section of the ICO Guide to the GDPR. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

'Old' Data

You should not be routinely keeping all the cases that you have assisted with. You must decide how long after you have closed a case to keep it for and after this period you should securely delete any files containing that data. This is the retention period mentioned above and you should do this regularly to show that you are complying with principle 5.

Reporting a personal data breach

The new Act will set a time limit of 72 hours of reporting a personal data breach to the ICO. It is expected that their online breach reporting system will continue. ALWAYS check the email address of the recipient before you send an email containing personal data as this is where the majority of breaches occur.

What Councillors must do in order to be compliant with the GDPR.

It is not possible to give a comprehensive answer to cover all possible situations in which a Councillor may find him or herself. The following five suggestions, if followed by a Councillor, are likely to avoid the major pitfalls (apart from not paying the annual fee) encountered by a Councillor in processing personal data as part of his/her office. It must be emphasised however that these are nothing more than a general guide and that there may be circumstances where more is required or where less is required. Each situation must be judged on its own facts according to the precepts of the GDPR. There are, moreover, bound to be further domestic regulations under the GDPR which will carve out exceptions.

(1) Get the individual's express consent to using his/her personal data in the way in which it is to be used. "Use" here includes recording and storing the data. Consent can be sought automatically.
(2) Do not share an individual's personal data with anyone else without first having obtained the express consent of the individual.
(3) Only use the personal data for the purposes for which you have obtained consent.
(4) When storing the personal data on anything, encrypt the data with a bitlock and a sophisticated password known only to the Councillor.
(5) Delete information when it is no longer needed. Upon ceasing to be a Councillor, delete all the personal data on any device belonging to or otherwise to be kept by the person who was the Councillor.

The General Data Protection Regulation (GDPR) Guidance for members

Do I still need to register under GDPR?

If you needed to register under the Data Protection Act 1998, then you will need to provide the ICO with information required and pay a relevant fee, (unless you are exempt) under the Data Protection (Charges and Information) Regulations 2018.

This doesn't mean everyone has to pay the new fee on the date that the new Regulations come into force on 25 May 2018. Data controllers who have a current registration (or notification) under the 1998 Act, do not have to pay the new fee until that registration has expired.

You can find more detail in the Guide to the Data Protection Fee. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/guide-to-the-data-protection-fee/

Penalties

You will be breaking the law if, as a controller, you process personal data, or are responsible for the processing of personal data, for any of the non-exempt purposes and you have either:

- not paid a fee, or
- not paid the correct fee.

The maximum penalty is a £4,350 fine (150% of the top tier fee.)

Further Information

This is a very brief overview of the new legislation. For more detailed guidance please visit the ICO website which has dedicated GDPR pages to assist you.

The ICO has produced a guide on the new GDPR which can be found here https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf