General Data Protection Regulation (GDPR)

Briefing for councillors

v1.0 8th May 2018

Introduction

This guidance is based on the draft issued by the Local Government Association (LGA) on 1st May 2018.

What is GDPR?

Data protection law is changing from 25th May 2018. The General Data Protection Regulation (GDPR) is a new, Europe-wide law that replaces the Data Protection Act 1998 (DPA) in the UK. It is part of the wider package of reform to the data protection landscape that includes the Data Protection Bill. The GDPR sets out requirements for how organisations will 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 DPA) 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.

What is the Data Protection Bill?

A Data Protection Bill (DP Bill) is also currently going through Parliament. The GDPR has direct effect across all EU member states and has already been passed. The DP Bill will bring much of GDPR into UK legislation which will be relevant when the UK leaves the EU and means organisations will still have to comply with GDPR and we will still have to look to it for most legal obligations. However, the GDPR gives member states limited opportunities to make provisions for how it applies in their country and another element of the DP Bill is the details of these. It is therefore important the GDPR and the Bill are read side by side.

What else does the DP Bill cover?

The DP Bill covers more than GDPR:

- 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

- A part that implements the EU's Law Enforcement Directive, part of the EU's data protection reform framework and separate from the GDPR. The DP 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.

- 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 Data Protection Act 1998 is being repealed so it makes the changes necessary to deal with the interaction between the Freedom of Information Act (FOI) / Environmental Information Regulations (EIR) and the DPA

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.

Personal data 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 (known as sensitive personal data under DPA) are those which are particularly sensitive:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic or biometric data
- health related data (includes social care)
- sex life or sexual orientation

New requirements

GDPR brings the following new requirements to organisations processing personal data:

- 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 individuals of their rights
- Ensure you have appropriate security measures in place to protect personal data you hold
- Routinely consider data protection at the beginning of a new initiative and when you review / update ('Data Protection by Design')

- Regularly review and delete ‘old’ data you no longer need
- Report any data breaches to the ICO within 72 hours

Six GDPR Principles

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

1. **Lawful, fair and transparency** - personal data shall be processed lawfully, fairly and in a transparent manner.

2. **Purpose limitation** - personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. **Data Minimisation** - personal data shall be adequate, relevant, and limited to what is necessary

4. **Accuracy** - personal data shall be accurate and, where necessary, kept up-to-date

5. **Storage limitation** - personal data shall be kept in a form that identifies the individual for only as long as necessary

6. **Integrity and confidentiality** - personal data shall be processed in an appropriate manner to maintain security and protect against unlawful processing or accidental loss

Record Keeping

You must keep certain records if you are processing either:

- more than occasional personal data (e.g. for complaints)
- any ‘special category data'

You need to record:

- the name and contact details of the Data Controller – yourself
- the purpose of your processing and legal basis for it e.g. to investigate complaints
- the categories of data you hold and the categories of data subjects e.g. name and address, email, medical information for constituents and complainants
- anyone you share the data with e.g. other Councillors / Council Officers / other services
- how long you keep data for e.g. 6 months after the case is closed
- what security you have in place to protect it e.g. password protection, only using secure Council provided email address, documents lockedin 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.

A Privacy Notice should include:

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

Rights of Individuals

Individuals can request Controllers take action to fulfil their rights. Each request received will be reviewed and actioned wherever possible. However, some action can be restricted or refused in certain circumstances and the Controller may not be able to comply with some requests received.

Individuals have the right to:

- be informed about what we do with your data
- access to the information we hold about you
- request rectification of any information about you that is incorrect
- Simple inaccuracies, such as address changes will be made, however, depending on the purpose for processing, some records, including statements and opinions may not be changed, but there will be the option for you to provide a supplementary statement which will be added to the file
- request records we hold about you are erased or "forgotten"
- restrict processing of your personal information if you have an objection to that processing, whilst your objection is investigated
- request any information that you have provided to us is given back to you in a format that you can give to another service provider if required - "data portability"
- object to processing of your personal information
- safeguards in relation to automated decision making and profiling

Security and keeping personal data secure

You should already be keeping personal data secure as this is a requirement of the DPA, a few reminders of some good security tips:

- only use your official email address

- be aware of your surroundings if you work in public areas so that you are not overlooked or overheard when working with personal data
- as now, always be careful with whom you share personal data, including with other councillors in multi member wards
- keep information for no longer than necessary – and securely dispose of it when you no longer need it
- don't leave documents containing personal data or unlocked computers / tablets unattended
- ensure the device you use is stored securely when not in use
- when emailing use the minimum amount of personal data necessary in order to make sense and avoid references to other identifiable people where possible

'Old' data and housekeeping

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 you need 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.

Personal data breaches

GDPR introduces heavier penalties for data breaches and non-compliance with GDPR, up to a maximum of £17 million for the most severe incidents. It also sets a time limit of 72 hours to report significant personal data breaches to the ICO, so it is important to report any suspected breaches of Council personal data as soon as possible.

A lot of breaches occur when the wrong recipient is sent information by email - ALWAYS check the email address of the recipient before you send an email containing personal data.

Notification and the Data Protection Fee

The requirement under DPA for Data Controllers to 'notify' the ICO about their data processing has been removed by GDPR. However some Controllers may still need to pay an annual 'data protection fee' of between £40-£2,900 to the ICO under the Data Protection (Charges and Information) Regulations 2018 unless an exemption applies. The ICO's guide to the Data Protection Fee provides more information about who needs to pay this fee.

Councillor's processing personal data **as members of the Council** do not need to pay a separate fee because it is the Council that decides how the personal data is used and processed, and the Council's fee covers this. However, Councillors processing personal data outside of the above definition **may need** to pay a fee to cover this processing, for example in a personal capacity. If you are unsure whether you need to pay a fee you can call the ICO helpline on 0303 1231113 for assistance, or check the ICO website.

Further Advice / Guidance

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, including their Guide to the General Data Protection Regulation (GDPR), and FAQs for local authorities.