General Data Protection Regulation. Overview for Councillors.

13th March 2018

On 25 May 2018, the existing Data Protection Act 1998 will be replaced by the new General Data Protection Regulations. Later this year, these Regulations will be adopted by the UK within a new Data Protection Act which is currently being considered by Parliament.

The new Regulations will enhance the rights of data subjects and give them more control over what happens to their personal 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 you need to put technical and organisational measures in place to protect the data from loss, wrongful disclosure or unauthorised access and to ensure the rights of data subjects are protected.

The Local Government Association will be publishing guidance and a e-learning training module in Feb/March 2018. The Council are reviewing its e-leaning provision and Members will be updated. (

The six general principles under the Regulations 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.

What is personal data under GDPR?

These include:

- an identifier, eg a name, email address, phone number
- personal identification numbers, eg 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 are those which are particularly sensitive regarding, race, ethnicity, political opinion, genetic or health related data and sexual orientation.

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.

As a Data Controller registered with the Information Commissioners Office you will need to comply with the new Regulation.

You should already be keeping personal data secure and only using your official email address to respond. You are already aware to be careful with whom you share personal data and to keep information for no longer than you need to. The new legislation 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 constituents) greater rights to control and access the data you hold about them.

New requirements:

- Keep a record of your processing activities to show your compliance with the legislation.
- Give a more detailed Privacy Notice when you collect personal data.
- Tell data subjects of their rights.
- Maintain your registration with the ICO – the fee is likely to rise.
- Delete 'old' data you no longer need.
- Report certain breaches within 72 hours.

Record Keeping:

To comply with the legislation you must keep certain records if your processing is more than occasional (eg 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 constituents and you should record (perhaps in a word document):

The name and contact details of the Data Controller – yourself;

The purpose of your processing and legal basis for it e.g. the consent of the data subject in order 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; and

What security you have in place to protect it, e.g. password protection, only using the EHC provided email address, documents locking in a cupboard , ensure and that no other persons can gain access to these systems.

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; you should therefore seek to obtain their signature and you should keep a record that they have given consent.

A Privacy Notice should include:

That you are the Data Controller and your contact details;

The purpose of processing and legal basis for doing so (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 for it to be deleted; and

To contact you if they have a complaint about how their data is handled and if it is not resolved to contact the ICO.

See example document attached below.

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 20 working days 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.

Please ensure that you verify the person’s identity prior to releasing any personal information.

They can also ask for their data to be corrected, moved, restricted or erased in certain circumstances. Please inform the Data Protection officer should you receive a request to do this.

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 provide the minimum amount of personal data necessary in order to make sense and avoid references to other identifiable people where possible.

'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 legislation will set a time limit of 72 hours for reporting a personal data breach to the ICO.. 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.

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.

Alison Stuart
Alison.stuart@eastherts.gov.uk

Example of a Privacy Notice For the Council:

Application for a Temporary Event Notice – Licensing Act 2003.

Data Protection Notice

East Herts District Council is a Data Controller and can be contacted at:

Wallfields, Pegs Lane, Hertford, SG13 8EQ . The Data Protection Officer is (*awaiting confirmation)* and can be contacted at the same address.

We are collecting your personal data in order to process your application under Licensing Legislation as we are the Licensing Authority.

Your data will not be shared with third parties but may be used for Council purposes, in order to prevent or detect crime, to protect public funds or where we are required or permitted to share data under other legislation.

Your data will be kept for 6 years in line with our retention policy.

You have the right to access your data and to rectify mistakes, erase, restrict, object or move your data in certain circumstances. Please contact the Data Protection Officer for further information or go to our website where your rights are explained in more detail. If you would like to receive an explanation of your rights in paper format please contact the Data Protection Officer.

Any complaints regarding your data should be addressed to the Data Protection Officer in the first instance. If the matter is not resolved you can contact the Information Commissioner's Office at: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF Tel: 0303 123 1113

If you do not provide the information required on the form then we will not be able to process your application for a licence.

For further information on our Data Protection Policies please go to our website.

Example of wording for Councillors:

I [*insert name*] am a Data Controller registered with the ICO. I can be contacted at [*inserted details address where you hold your surgeries, email address*]

I am collecting your personal data in order to progress your [*insert details of why you are collecting the data]*

Your data will not normally be shared with third parties but may be used for other purposes, in order to prevent or detect crime, to protect public funds or where I am required or permitted to share data under other legislation. [*use if going to share information with the Council][if the matter is a complaint use the following: in order to progress your complaint I will need to share your data with the appropriate Council Officer, in order for me to do this I will need your consent, if the personal data is classed as being within the special categories of personal data I will need you to give your consent in writing. You can withdraw your consent at any time, the Council and I will not process your personal information from the time you withdraw your consent and will delete your data safely and securely in line with the retention guidance.]*

Your data will be kept for 6 months from the date of the completion of your enquiry/complaint in line with the Council's retention policy.

Your personal data will be kept [*insert details of security measures taken i.e. password protected document, locked cupboard etc.*]

You have the right to access your data and to rectify mistakes, erase, restrict, object or move your data in certain circumstances.

Any complaints regarding your data should be addressed to [*insert your name*]. If the matter is not resolved you can contact the Information Commissioner's Office at: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF Tel: 0303 123 1113

For further information on Data Protection Policies please go to the Council's or the Information Commissioner's website.