

Corporate Information Management Unit - Guidance

General Data Protection Regulation (GDPR)

Briefing for councillors

v1.0 8th May 2018

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 The Data Protection Act 1998 is being repealed so it makes the changes necessary to deal with the interaction between the Freedom of Information Act (FOI) / Environmental Information Regulations (EIR) and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 0 Tw 19.4(.7(e))TJel)-0ppln sedifiep.]TJelndi0 Tdre()

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.

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 a Td [(3er)6(t)-7-8.1(e3er)6(Dt)4.2(i)--8(c).3er Pi Tc 0 Tw (.)Tj 20 T18