SLCC
For Local Council Professionals ®
50 YEARS
1972-2022
ANNIVERSARY

Update on GDPR
Clerks & Councillors Personal Devices

What is Data

- **Personal data means any information relating to an identified or identifiable natural person (living Person) (Data Subject)**

- Name
- Identification number
- Location data
- An online identifier or one or more factors specific to the physical physiological, genetic, mental, economic, cultural, or social identity of that natural person

What is consent under GDPR?

Consent has to be specific and informed – using a default opt in and requiring an affirmative action to opt out will not be compliant under GDPR.

Blanket or generic consent is not considered to be consent – “Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case” (Recital 43)

The act defines explicit consent as:

- A clear affirmative act
- Freely given
- Specific
- Informed
- An unambiguous indication of the data subjects agreement
- Consent required for each purpose of processing
- Data Subject shall have the right to withdraw his or her consent at any time
- Controllers must keep records of consent & the context it was provided
- Controllers must ensure consent can be withdrawn as easily as it was given
- The withdrawal of consent must shall not affect the lawfulness of processing based on consent before its withdrawal.
- **If data is held for legislative reasons, it cannot be deleted as the legislation takes precedence.**

The Law

Integrity and confidentiality principal of GDPR states the organisations must process personal Data in a manner that ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Therefore, Councils must have appropriate security measures in place to prevent personal information the organisation holds from being lost, stolen or used inappropriately.

This can pose a challenge where a Councils information is being accessed, stored and used on a **personal device**. In order to compile with the integrity and confidentiality principal in GDPR, organisations must remain in control of its personal information **regardless of who owns the device the work** is carried out on.

Council issued devices

This is generally the most secure option, but it is also the most expensive. **The Risk should be assessed by the Council.**

Things you should consider:

- Ensure that the devices can be supported and updated remotely.
- Ensure that mechanisms are in place to prevent data from being extracted from the device, e.g. data loss prevention technology.
- Ensure that remote access authentication is securely configured and consider using multi-factor authentication for remote access.

Use your own device, but access Council software

This is a more cost-effective option, but comes with some security risks.

Things you should consider:

- Consider using multi-factor authentication for remote access.
- The device owner’s data and the organisation’s data should be separate. Councillors and Staff should not be able to inadvertently or deliberately move the organisation’s data into their personal storage on the device or onto separate personally-owned devices.
- Organisations need to be aware that the device’s security posture may be compromised and plan accordingly, e.g. out of date and unpatched operating system or security software.

Use your own device - This approach the riskiest!

Things you should consider:

- Out of date software (including the operating system) may be vulnerable to exploitation including loss or compromise of personal data.
- Devices are likely to be shared between family members. Other family members may see personal data that they should not have access to.
- Data is unlikely to be encrypted on the device and may be vulnerable in the event of loss or theft of the device.
- Inadequate access control, e.g. weak laptop passwords, may result in personal data being easy for unauthorised individuals to access.
- Data can easily be moved to other insecure storage (personally-owned USB sticks and external hard drives), increasing the potential for loss.
- Councillor & Staff usage of insecure methods to communicate, such as personal email accounts, may result in compromise of personal data.

Councils should consider these security risks and put mitigation methods in place to avoid data breaches.

For example, provide your Councillors and staff with guidance on how to secure their device by keeping software up to date, give advice on strong passwords and minimise the storage of personal data on their device and insecure storage such as USB sticks.

You should every year action GDPR training to ensure Councillors and staff understand when and how they can internally report potential personal data breaches.