# General Portable Storage Device Recommendations

An Coimisiún um Chosaint Sonraí
Data Protection Commission

One of the main obligations under the General Data Protection Regulation (GDPR) for organisations which process personal data ('controllers'), is that they must do so in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing (including theft, destruction or damage, or disclosure) using 'appropriate technical or organisational measures'. This is sometimes referred to as the principle of 'integrity and confidentiality' or the 'security principle'.

This obligation is an important one, which controllers should be cognisant of, particularly those who utilise or store sensitive personal data. Whether or not an organisation has appropriate technical and organisational measures in place to ensure the security of the personal data they process is one of the first questions the Data Protection Commission (DPC) is likely to ask in the event of a personal data breach or the exercise of the DPC's investigative powers. Controllers can also consult our guidance for controllers on data security when assessing the appropriate security measures they need to implement.

The decreasing cost of electronic storage and processing has greatly contributed to the large increase in the quantity of personal data stored in recent years, often on portable storage devices, which gives rise to particular security challenges for the organisations responsible for that stored data.

To ensure that they have appropriate technical and organisational measures in place, any organisation utilising portable storage devices to store or transmit personal data should consider the particular risks associated with the use of such devices, such as loss or unauthorised access, and ensure that they have internal policies and technical measures which mitigate these risks.

## Recommendations for the Use of Portable Storage Devices

The recommendations below should assist controllers with their own internal policies on the usage of portable storage devices, including USB keys, external hard drives, micro-SD cards, or even the internal memory on portable devices such as smartphones, tablets, and laptops. These recommendations are general in nature and the appropriate policy to implement may vary depending on the nature and circumstances of the data controller and storage in question.

☑ Staff within an organisation should *not* utilise their own personal portable storage devices for storing personal data related to their work. This position should be part of the organisation's internal policy and communicated to all personnel.

- ☑ Only whole-drive encrypted, passphrase-protected portable storage devices, issued by the organisation to authorised personnel, should be utilised. No unauthorised device should be used on any of the organisations' systems.
- ☑ Organisation-issued portable storage devices should not be used on personal machines or machines that do not belong to the organisation.
- ☑ Organisations' portable storage devices should be returned when personnel cease employment with the organisation.
- ☑ To prevent data leakage, organisations should operate restricted permissions, to restrict staff from copying data to portable memory devices.
- ☑ Data storage or copying of personal data onto a portable storage device must only be done by an authorised individual in the performance of official duties. This may be achieved by utilising a data loss prevention solution.
- ☑ Portable storage devices should utilise password protection, incorporating strong passwords – which should include a minimum of twelve characters and contain one or more of the following:
    - Letters (upper/lower case)
    - Numbers (0-9)
    - Symbols (&, *, @, €, $, etc.)
    - Punctuation (?, ", !, etc.)
- ☑ Enforce USB key scanning for all computers whenever a USB key is plugged in. This can help ensure that no malware or malicious programs are present on the USB key.
- ☑ All data transferred to a portable storage device should be backed up.
- ☑ Ensure personal data stored on a portable storage is only stored for a short period of time and deleted when no longer required.
- ☑ Where possible, data transferred to a portable storage device should have a expiry.
- ☑ Where possible, utilise portable storage devices which support, through a remote administration tool, a remote disable or wipe facility.
- ☑ If a portable storage device is lost, organisations should be able to access and analyse the latest secure backup to review what was lost and assess the potential risk.
- ☑ When not in use, portable storage devices should not be left unattended and should be securely locked away.
- ☑ When in transit, portable storage devices must not be left unattended and must remain in the control of an authorised individual.
- ☑ An asset register should be maintained of all organisation portable storage devices and the authorised personnel in which they have been issued to.
- ☑ Regularly audit USB devices to ensure that only documents in compliance with acceptable usage are being stored.
- ☑ Organisations should know their assets, and have a precise count of the portable storage devices in use within their staff. These should be listed by owner and use.
- ☑ Only purchase and utilise portable storage devices from reputable and recognised manufacturers and re-sellers.

Personnel who utilise portable storage devices should be made aware that they have a duty of care to ensure all personal information is held securely at all times. Personnel should also be made aware that the loss of personal data may be considered a serious risk, with potential implications for the organisation under its GDPR obligations, particularly regarding data breaches.

As noted above, every controller and processor acting on their behalf has an ongoing obligation to comply with data protection law, specifically under the Data Protection Act 2018 and the GDPR, which includes a duty to implement appropriate technical and organisational measures to ensure security for personal data and to maintain a record of processing activities which contains documentation of the measures applied.

## Breach Notification Requirement

Loss of portable storage devices is a common theme in many data breach notifications, where devices containing personal data, such as USB-keys, or laptops, are stolen or misplaced. Organisations are reminded of their obligation under the GDPR to report personal data breaches to the relevant supervisory authority (in Ireland, the DPC), where the breach presents a risk to the affected individuals.

Organisations must report personal data breaches to the DPC within 72 hours of becoming aware of the breach. Where a breach is likely to result in a high risk to the affected individuals, organisations must also inform those individuals without undue delay. Further guidance on breach notifications can be found on the DPC's website.