7/ Secure Data Storage and Deletion

Things to consider

Although you may have a user password, data on devices may be accessible to third parties who obtain physical access to the device.

- Better resourced adversaries are not deterred by a strong user password: in most cases, **data is stored in a readable format** on hard drives, mobile devices, and USB keys, unless additional measures have been taken to protect it.
- Files deleted via the normal 'Recycle Bin' option **do not disappear** after the Recycle Bin is emptied. Instead, they are assigned by the Operating System as **'free space'**. This means that the space on the drive can be overwritten by new data. However, until that point, the data remains recoverable.
- Deletion of data on modern flash storages like USB drives, mobile phones, or solid-state hard-drives (SSDs) is technically **nearly impossible** without overwriting all free space after the deletion of the respective data.

Protection tactics

- Remember the basics: ensure that your user accounts on your computer have **strong passphrases**, and that your mobile devices have **PIN or passwords** activated.
- Regularly **wipe your 'free space'**: There are programs that overwrite 'free space' on hard drives, and which can delete old and temporary files. However, there is no guarantee that data on devices with SSD hard drives can be effectively overwritten.
- There are some options to protect your data through **encryption**. Be aware that in some contexts, this may be legally restricted or may draw attention to you.
- Consider **full disk encryption**, which means encrypting all of the data on a particular device or drive partition, or creating encrypted folders on your device. Many smartphones and some computers come with this option; see the website for more up-to-date information regarding this.
- In addition, or as an alternative, you can use **encryption software** to create encrypted volumes. This involves creating a space, like a folder on your device, where sensitive data can be stored.
- Accept only **encrypted external drives** such as USB keys. This implies that they are only readable on devices with the right encryption software installed and with a password created upon encrypting the device.