Data protection by default in practice

Best practices on data protection by default

Criterion 1: Minimum amount of personal data

- **The less data, the better** Data minimization refer to any way of reducing data collection and further processing of data (following not only a quantitate but also a qualitative approach).
- **Granular collection of data on the basis of necessity** multiple sub-purposes govern different of the processing.
- **Use of privacy enhancing technologies:** Data minimisation can in several instances be achieved by the use of security and privacy enhancing technologies,

- **Different minimum per purpose** the best practice for the controller is to re-assess defaults in all cases (apps, messengers)

- **Minimizing the risk** for determining the minimum amount of personal data,

- **Considering all copies and types of data** reducing temporary copies or transfer of data as much as possible with respect to the purpose.

Criterion 2: Minimum extent of the processing of the personal data

- **The less processing, the better** the requirement for 'minimum extent' does not mean to reduce the number of operations, but to minimise the risk for the rights and freedoms of natural persons.
- **User empowering tools** The limitation of the extent of the processing is closely interlinked with the provision by the controller of proper tools

Criterion 3: Minimum period of the storage of the personal data

- **Storage – the shorter, the better** for the personal data the storage period shall be minimised.

Criterion 4: Minimum accessibility of the personal data

- **Restricting access on the basis of necessity** The requirement of minimum accessibility is clearly relating to access policy and access control
- **Limiting ways of sharing** the different possible ways of data sharing should be assessed and, wherever possible, minimized by the controller.
- **No public by default without active intervention** aims at preventing personal data from being made public by default

Defaults and usability

Users can easily go back to default and applications stay easy to use after having changed the pre-configured "data protection by default" setting, users should be able to easily go back to this default setting. Determining the 'correct' defaults is in fact a direct matter of usability