

04 DATA MINIMISATION

What is needed?

The capacity of computer systems to store and process personal information has been constantly increasing in recent years. As the mass of personal information increases, so do resulting threats to privacy and security.

Data minimisation is an essential principle of data protection. It establishes that data collected and processed should not be retained or further used unless this is necessary for purposes that were clearly stated in advance.

Before starting to process personal data, controllers should ask themselves: “Do we need this? What for? And for how long?” The existing 95 Directive already contains the principle of “not excessive data collection”, but it is not very well observed. This principle is being clarified and strengthened by Article 5 (c) of the proposed General Data Protection Regulation.

negative amendments

Amendments 824, 825, 826 and 827 seek to delete the notion that collection of data should be limited to the minimum necessary and replace it by the wording « not excessive », which is more vague and which will not provide a much-needed improvement of the current legislation. The vague concept of “not excessive” is hard to enforce and opens the door for unlimited retention periods, unexpected re-use and other forms of abuse.

positive amendments

Amendments 752 and 753 introduce new provisions to define « data protection by default and by design » and to clarify that these principles should also include data minimisation.



LAW ENFORCEMENT ACCESS

When it comes to personal and intimate information held by companies about our private lives, it is essential that these data are kept to a minimum; otherwise we risk more abuse and increase the loss of control over how our personal data are used, shared and sold.

The European data protection regime is applicable to all companies providing services in the EU. Data minimisation can therefore be a good step towards fewer data being stored, more control over what data is stored and a corresponding reduction of the risk of surveillance from (foreign) governments and more control over one’s personal data.