

SUMMARY OF DATA PROTECTION PRINCIPLES

The list below gives a quick overview of generally recognised data protection principles. You will be able to find all or most of them in data protection rules in the EU. It is for you as a controller to follow them and to be able to demonstrate that. They do not replace the advice given in these guidelines, but provide the philosophy behind them.

1. Personal data shall be processed fairly and lawfully.

You need to make sure that you have a lawful reason for processing personal data. This could be that the processing is necessary for the performance of the tasks of your institution attributed to it by law (including necessary internal administrative activities). Fair processing means telling people about what will happen with their data and sticking to what you told them.

2. Personal data shall be processed only for specified explicit and legitimate purposes, and shall not be further processed in a way incompatible with those purposes.

Explicitly determine why and how you process personal data. Do not use them in a way that is incompatible with that initial purpose.

3. Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed.

Think about which data you need to achieve your determined purposes and process those data categories, not more.

4. Personal data shall be accurate and, where necessary, kept up to date.

Make sure that the data you process are accurate - inaccurate data can lead to taking wrong decisions. Where relevant, make sure that the data are up-to-date.

5. Grant the rights to access and rectification

Persons have the right to access their personal data processed by your institution and to have incorrect data rectified. Make sure that it is easy for them to exercise these rights. This can also help you in making sure data are correct and up-to-date.

6. Personal data processed shall not be kept for longer than is necessary.

Think about how long you need to keep the data and then keep for them for that duration, but not longer.

7. Keep personal data safe

Do a risk assessment and take appropriate security measures based on the state of the art, the risks of the processing and the cost of implementation.

8. Rules on transfers

Make sure you follow the specific rules for transferring personal data to third parties, especially when transferring outside the EU.