Useful points and questions on data protection

Main lines:

- Think about what you need to fulfil your business needs and limit yourselves to it.
- Define what you do, document it.
- Tell people about it and respect their rights.

Some useful questions:

- What exactly do we want to do and why?
- Why are we allowed to do it?
- What data do we need to do it and for how long?
- Who needs to have access to the data?
- How do we make sure it's not used otherwise?
- How do we tell people about it and give them access to their data?
- How do we document all this?
- Want to know more? Need guidance? Talk to your Data Protection Officer. Document.

Why tell people? So that they can:

- understand which of their data are processed and how;
- verify the quality of their own data;
- exercise their other data protection rights (access, rectification, erasure, restriction of processing, notification of rectification, erasure, restriction of processing, data portability, objection, not to be subject to a decision based solely on automated processing, including profiling).

Data protection factors when publishing personal data:

- Am I obliged to publish? May I publish? (legal basis)
- What can I publish? (data minimisation)
- How do I tell the individuals concerned? (information)
- How do I make sure the data is correct? (accuracy)

Guiding Questions on fairness

- Can people expect this to happen, also if they don't read the information you provide them with?
- In case you rely on consent, is it really free? How do you document that people gave it? How can they revoke their consent?
- Could this generate chilling effects?
- Could this lead to discrimination?
- Is it easy for people to exercise their rights to access, rectification, etc.?

Guiding Questions on transparency

- How will you tell people about your processing?
- How do you make sure the information reaches the persons affected?
- Is the information you provide complete and easy to understand?
- Is it targeted to the audience? E.g. children may require tailored information
- In case you defer informing people, how do you justify this?

Guiding Questions on purpose limitation

- Have you identified all purposes of your process?
- Are all purposes compatible with the initial purpose?
- Is there a risk that the data could be reused for other purposes (function creep)?
- How can you ensure that data are only used for their defined purposes?
- In case you want to make available / re-use data for scientific research, statistical or historical purposes, what safeguards do you apply to protect the individuals concerned?

Guiding Questions on data minimisation

- Are the data of sufficient quality for the purpose?
- Do the data you collect measure what you intend to measure?
- Are there data items you could remove without compromising the purpose of the process?
- Do you clearly distinguish between mandatory and optional items in forms?
- In case you want to keep information for statistical purposes, how do you manage the risk of re-identification?

Guiding Questions on accuracy

- What could be the consequences for the persons affected of acting on inaccurate information in this process?
- How do you ensure that the data you collect yourself are accurate?
- How do you ensure that data you obtain from third parties are accurate?
- Do your tools allow updating / correcting data where necessary?
- Do your tools allow consistency checks?

Guiding Questions on storage limitation

- Does EU legislation define storage periods for your process?
- How long do you need to keep which data? For which purpose(s)?
- Can you distinguish storage periods for different parts of the data?
- If you cannot delete the data just yet, can you restrict access to it?
- Will your tools allow automated erasure at the end of the storage period?

Guiding Questions on security

- Do you have a procedure to perform an identification, analysis and evaluation of the information security risks possibly affecting personal data and the IT systems supporting their processing?
- Do you target the impact on people's fundamental rights, freedoms and interests and not only the risks to the organisation?
- Do you take into consideration the nature, scope, context and purposes of processing when assessing the risks?
- Do you manage your system vulnerabilities and threats for your data and systems?
- Do you have resources and staff with assigned roles to perform the risk assessment?

