Oh noes, a lawyer

But what is Privacy by Design?

Who is this lawyer?

- A privacy professional with several years of experience in the field.
- Vice chairperson at the Swedish Data Protection Forum (Forum för Dataskydd)
- Owner and senior legal consultant at Data Law Center

Data Law Center

Data Law Center ("DLC") is a legal consulting firm that focuses on legislation on information and digitalization. The main practice areas are:

- Data protection (Privacy)
- Information security
- Swedish national security
- Swedish Govermental legislation

Agenda

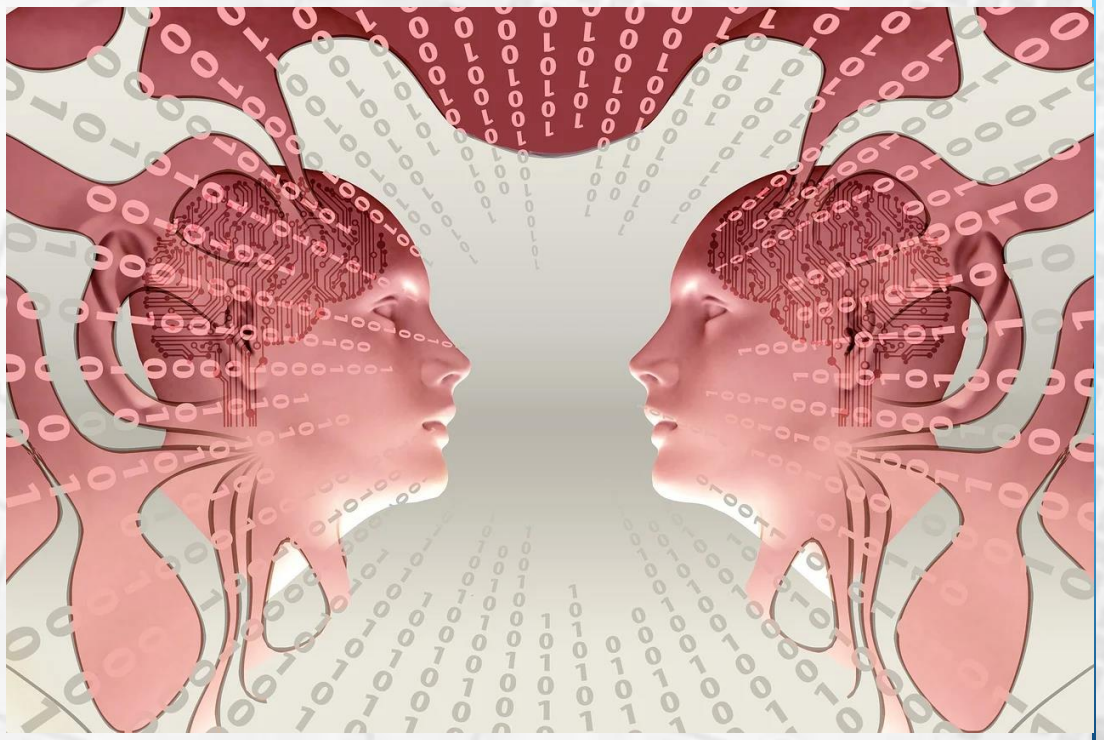
- What is Privacy by Design?
- How do we apply it in development of projects
- In depth
  - Personal data
  - Cloud services
  - Transfers out of EU/EES

Privacy by Design (PbD)

- A term coined by the Canadian Dr. Ann Cavoukian
- Implemented in GDPR as Data Protection by Design and by Default (DPbDD)

Data Protection by Design and by Default (DPbDD)

- A legal concept of obligations.
- The obligation is in its basic form to implement measures that makes the privacy a core feature *with regards to:*
  - the current state of the art
  - the cost of implementation
  - the nature, scope, context and purposes of processing
  - risks for data subjects

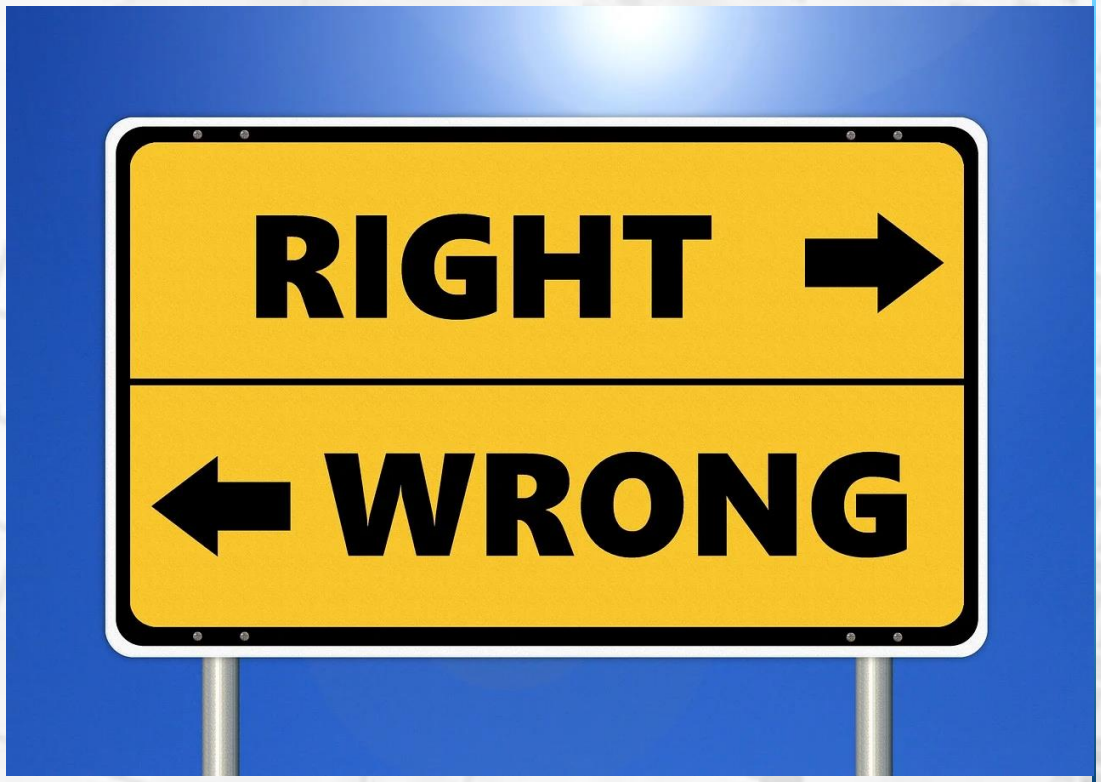


But what does it (DPbDD) mean?

- It means that you are required to implement safeguards when you process personal data in order to conform to **data protection principles** and protect data subjects' **rights and freedoms**.

Data Protection Principles (art.5 GDPR)

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability



EU Charter of Fundamental Rights (Rights and freedoms [recital 4])

The processing of personal data should be designed to **serve mankind**.

The right to the protection of personal data is **not an absolute right**; it must be considered in relation to **its function in society and be balanced against other fundamental rights**, in accordance with the principle of proportionality. This Regulation **respects all fundamental rights** and observes the freedoms and principles recognised in **the Charter as enshrined in the Treaties**, in particular the respect for private and family life, home and communications, **the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.**

But what about risk?

Data protection is fundamentally about putting yourself in the place of the individual (data subject) and on this basis safeguarding his **reasonable expectations of consideration** for his individuality (privacy).

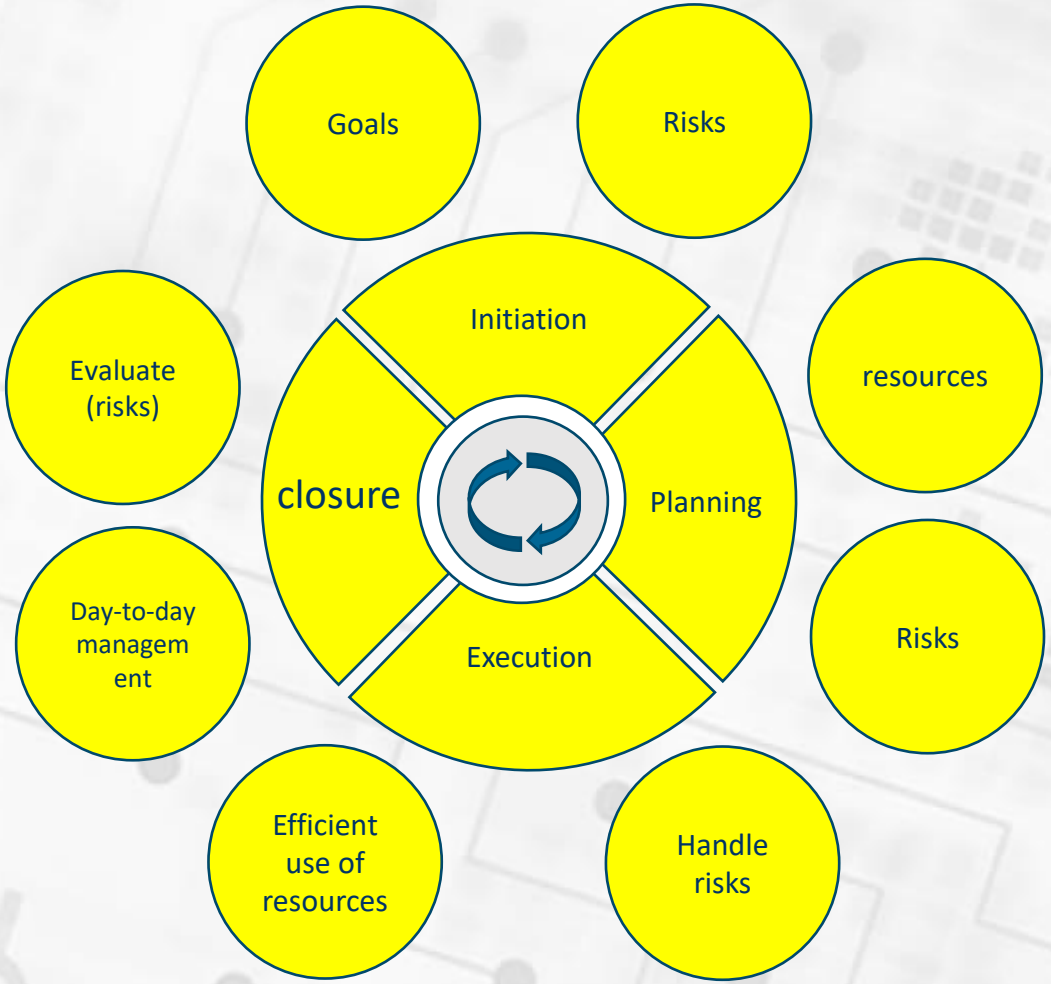
Basically, in simple terms DPbDD, is about:

- the process of assessing and determining the protection that personal data needs based on the risks involved.
- in the case of additional processing is not necessary for the basic processing, the additional processing shall not be carried out without the choice of the data subject, unless legitimate reasons exist otherwise.

PDbDD during project development

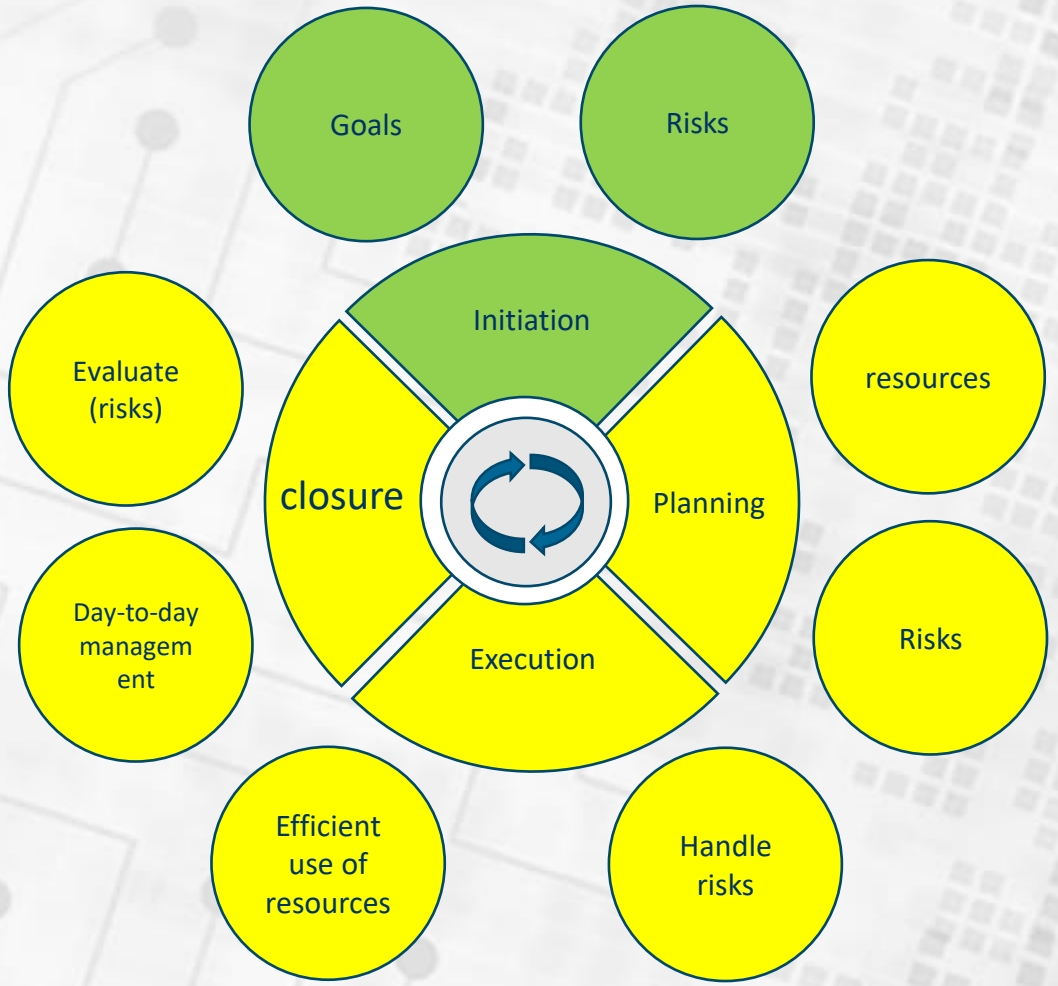
- Different models for projects are used within different organizations. In this context, the project model refers to the following – with a particular focus on data protection elements.
- Initiation
  - Examine the benefits,
  - current status,
  - risks and
  - planning for success.
- Planning
  - How will the project be implemented,
  - Costs,
  - Resources and
  - Risks.
- Execution
  - Deliver on plan,
  - Manage risks and
  - Use resources efficiently.
- Monitoring, & closure
  - Evaluate (risks),
  - Constant learning and
  - Day-to-day management.

A representation of project development



Initiation of projects

- If the product of a project will process personal data, in our experience the following should be included in the initial feasibility study.
- Clarification of current and desired personal data processing.
- Initiated risk assessment, pre-impact assessment or other risk assessment process.
- Pay attention to risks (this is central).

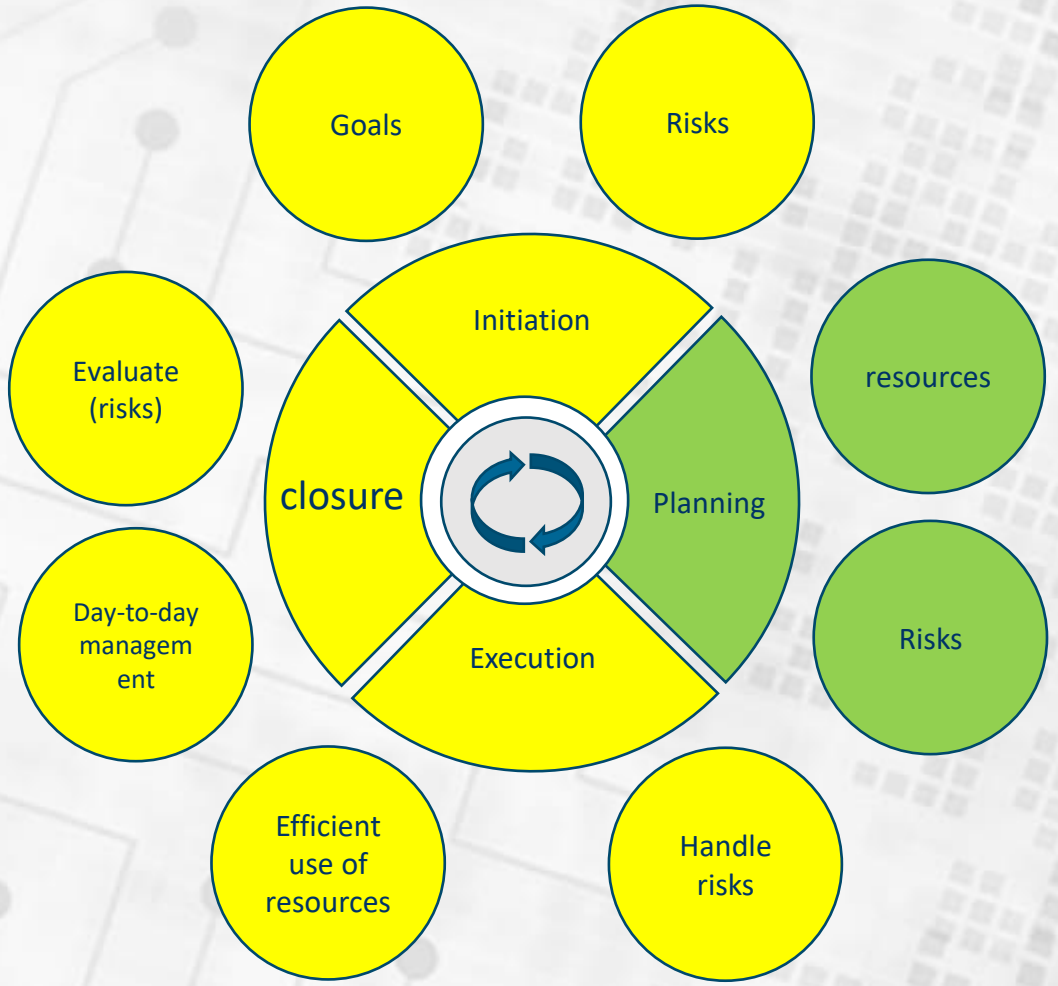


Planning of projects

In the planning step, it is the crucial decisions that are made for how the implementation should take place.

In this respect, most of the risk assessments should normally be carried out in order to ensure that implementation and implementation are carried out appropriately.

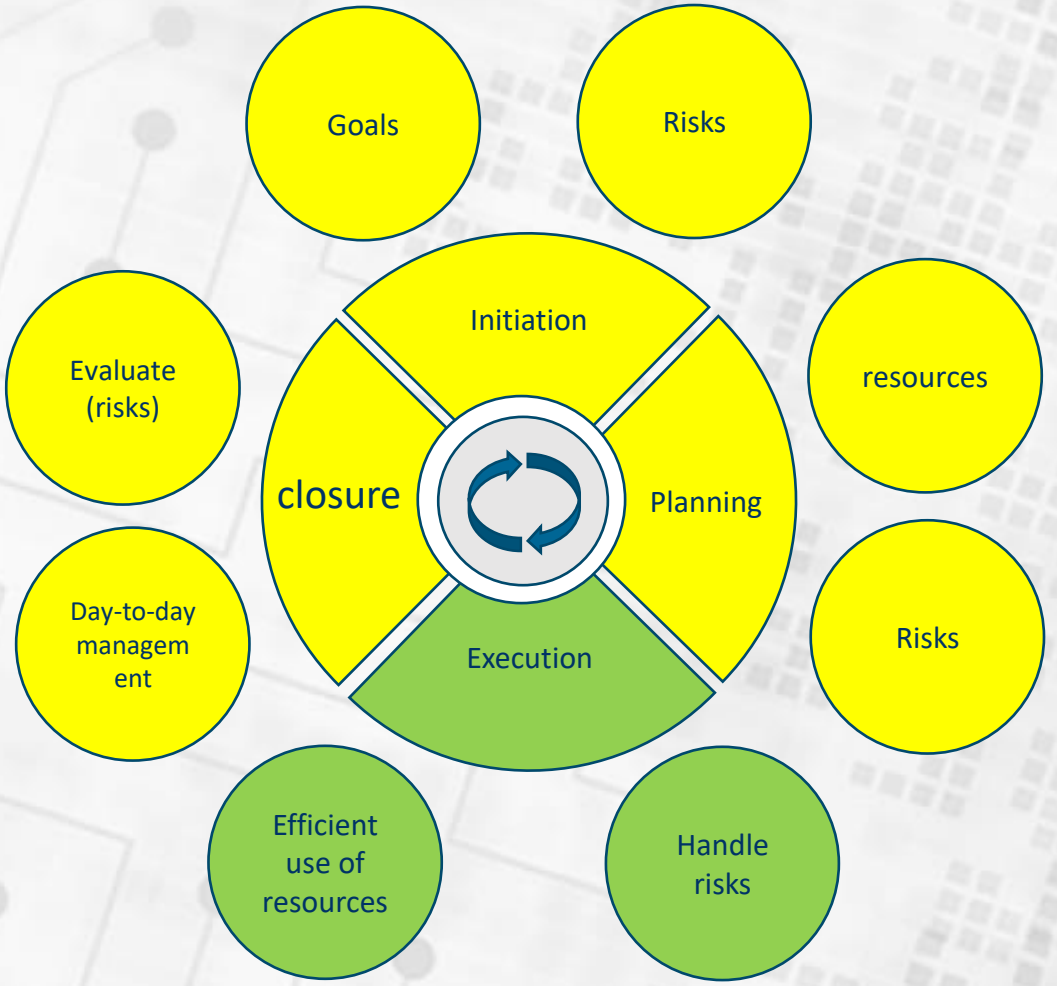
Here, the Data Protection Officer or privacy competence should normally have the opportunity to comment on the solutions.



Execution of projects

Here, the work is carried out by the resources allocated. Normally, new issues are discovered that have not been taken care of in the preliminary study or during the planning step and may be dealt with on an ongoing basis. For example, it may turn out that the selected supplier has fourth-tier dependence which might be non-compliant (i.e. Illegal third world transfer).

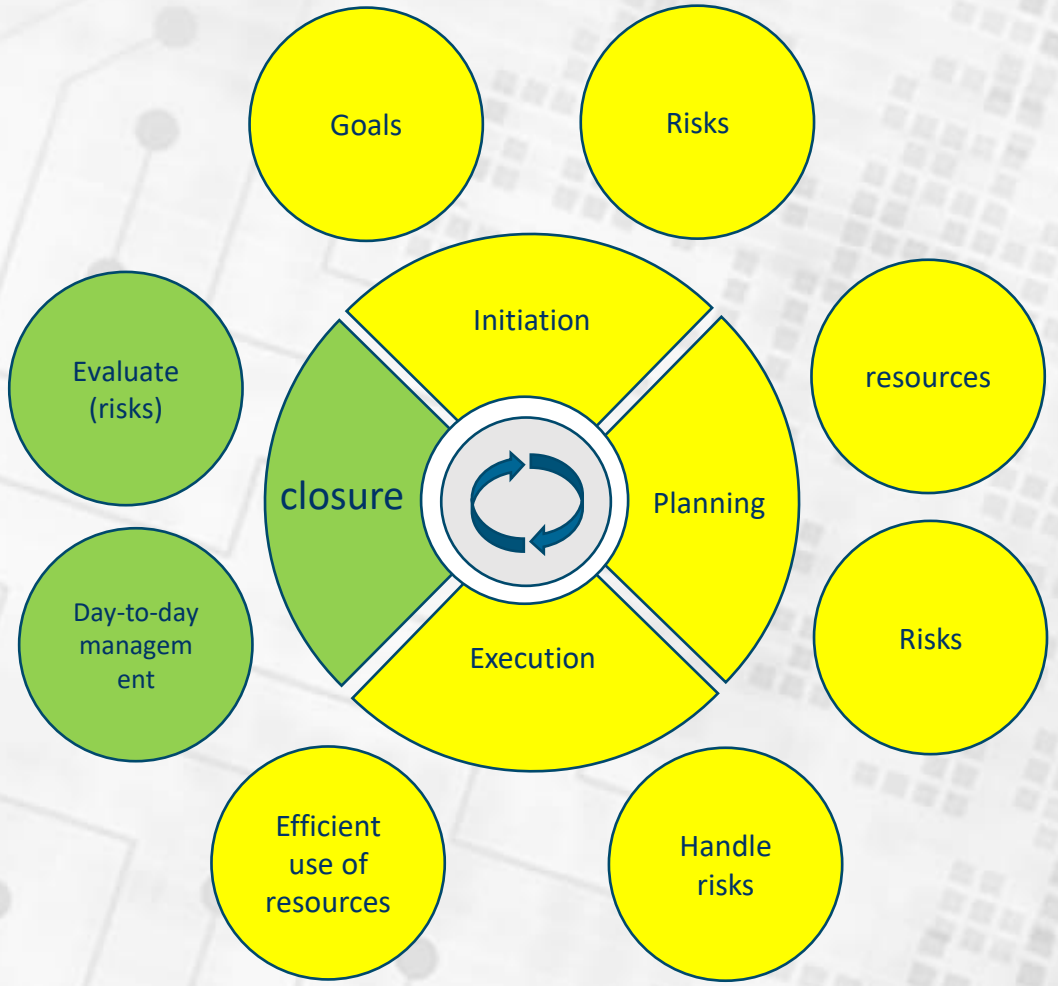
In this step, data protection officers are normally not involved other than possibly at a strategic level.



Closure of projects

In the final part, the project is often handed over to day-to-day management. It is just as important to resource management as the project. There are often outstanding tasks from projects that need to be handled in day-to-day management. In this step, it is regular information management that hopefully takes place under a management system.

Here, analyses are made at given intervals that the solution is still suitable. Often through the review of, for example, system management plans.



In depth: Personal data

- A wide legal term
- Anything that can lead to the indentification of a living person.

What is personal data?

Special categories of personal data

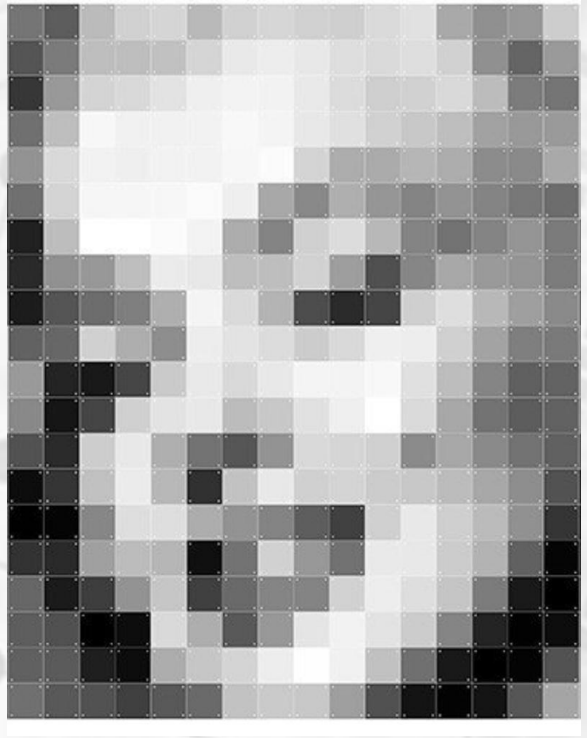
- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- membership of a trade union
- health
- a person's sexual life or sexual orientation
- biometric data that unequivocally identifies a person
- genetic data

Is this personal data?

- The name Anders Andersson? (Maybe)

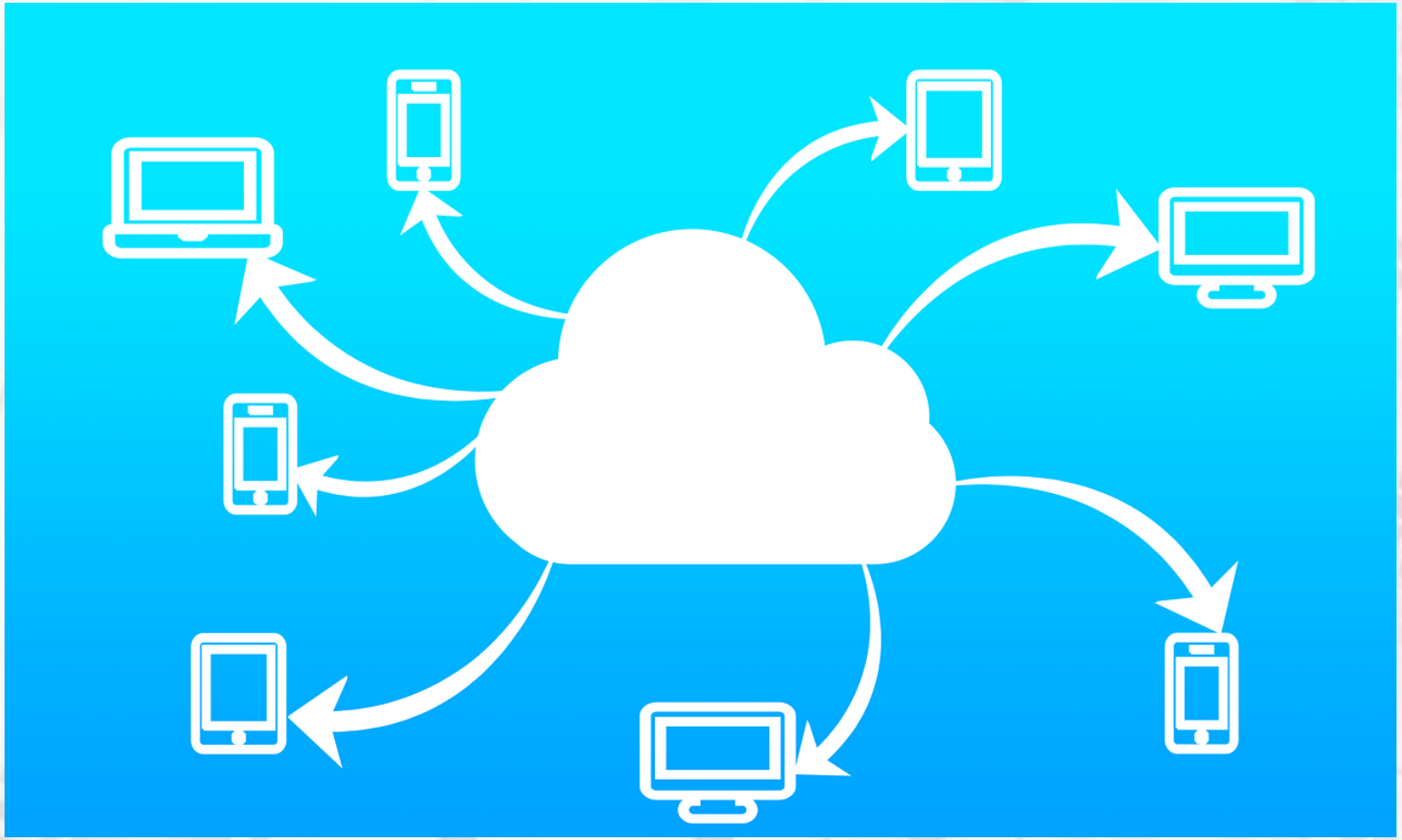
- A picture of a hand? (Maybe)

- The lawyer in the room that spoke about privacy yesterday? (Yes)



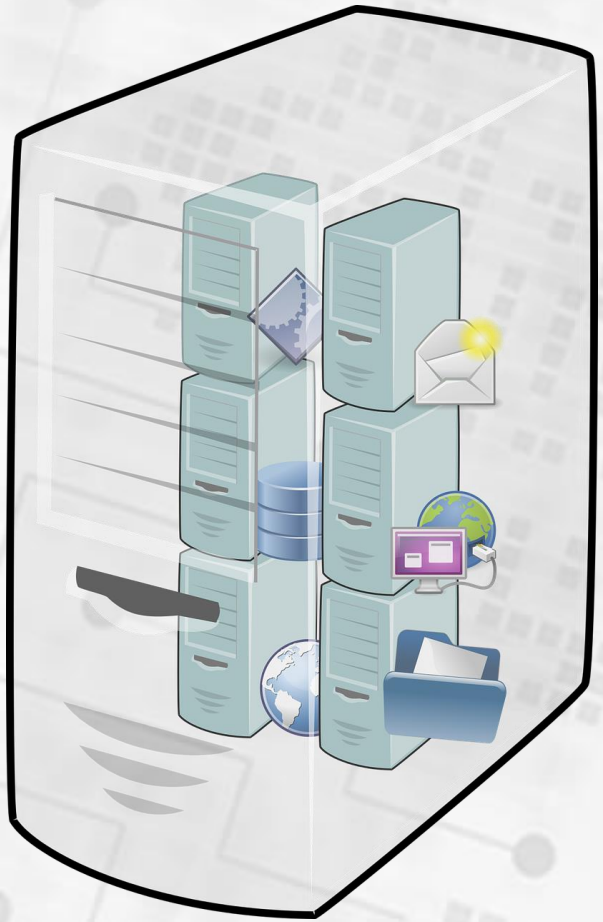
- Not a living person.

In depth: Cloud services



Cloud services

- A cloud service is when another organization sits on data belonging to another organization. Normally, cloud service providers become personal data processors in relation to the person who has hired out the data management.



Cloud services

Legal issues:

- Safety requirements (internal or legal requirements)
- Confidentiality
- Vendor review
- Right of inspection

(cf. Art. 28 GDPR)

Cloud services

Cloud services are in many cases in themselves unproblematic, but:

- Many suppliers are unfamiliar with safety requirements and have standard solutions.
- Third country problems (coming later)

In depth: Transfers out of EU/EES

Transfers out of EU/EES

The possibility of transfers to what are called third countries, i.e. non-EU/EEA cooperation, is limited. The main rule is that these are prohibited.

This is because the right to privacy is considered human rights based on:

- the protection of private and family life (Article 7 Charter of Rights);
- protection of personal data (Article 8 Charter of Rights)
- the right to effective remedies, such as courts (Article 47 Charter of Rights).

Transfers out of EU/EES

There are exceptions that make it possible to disclose personal data in certain cases, for example, in the case of personal data.

- Adequacy decisions
- European Commission Standard Contractual Clauses (SCC)
- Legally binding and enforceable instruments between public authorities and public bodies
- Approved codes of conduct
- Contractual clauses or provisions specially approved by the supervisory authority in the individual case
- Previous common exemptions (no longer lawful):
- Safe harbour
- Privacy shield

Transfers out of EU/EES

- The aim of restricting the possibilities for third-country transfer is to ensure the protection of human rights (see previous picture).

- The rules on third-country transfers shall therefore be applied in such a way as to ensure that the level of protection afforded by the GDPR is maintained regardless of where personal data is processed.

Transfers out of EU/EES

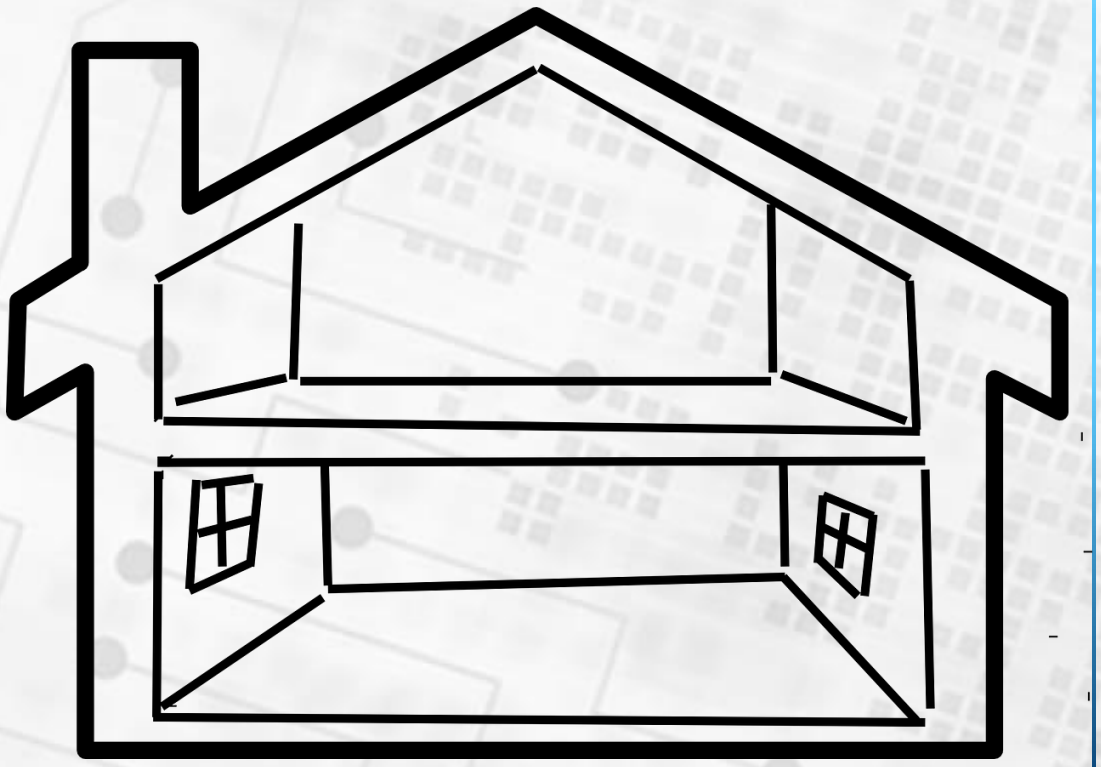
- In the absence of a adequacy decision, the organization wishing to transfer the data shall ensure that at least the same level of protection is obtained in the third country. To achieve this, a model with a number of steps can be used.

1. Map transfers
2. Check the basis of the transfer
3. Analysis of the third country by doing a transfer impact assessment (TIA)
4. Implement complementary protection measures to remedy any differences in protection
5. Take any formal action necessary to make measures legally binding
6. Evaluate transfers

Transfers out of EU/EES internal considerations

Before a processing is outsourced to the external supplier, consideration should be given to how the conditions appear to exercise the necessary control over the transfer and processing internally. Simply because external resources carry out essential parts of a processing does not mean that the organization can waive responsibility legally. Examples of appropriate considerations before third country transfer:

- What time is needed on an ongoing basis to carry out the necessary data protection checks?
- What are the conditions for dealing with the shortcomings that arise continuously in a satisfactory way?
- What added value does the transfer create in relation to the risks of the treatment?
- Is there a plan to suspend cooperation if the risks become too great (exit plan)?
- In parallel, is there a continuity plan internally and with the partner if the processing is critical for the business or the data subjects?



Transfers out of EU/EES external considerations

- If suppliers and third parties are long-term partners, it is important to keep up to date with how they work with their treatments and to have dialogue about this. It is then also important to ensure that their considerations are in line with your organization's requirements. Examples of appropriate considerations related to external vendors.
- How do they carry out the transfer today?
- Do they take greater legal risks than your organization? If yes, are those risks acceptable?
- Do they review their subcontractors for risks associated with the processing?
- Does the subcontractor have their own non-EU/EES dependencies?
- Are there any plans to change the transfers?
- Have they done the necessary risk and vulnerability analyses related to this?
- Have they done the necessary risk analyses related to data protection?
- Are there procedures for implementing the above and are they followed in practice?
- What does legal and data protection maturity look like?
- Are legal risks taken into account in business development, etc.?
- Is data protection actively worked on the basis of control and management processes?

Contact information

Data Law Center

Mattias Gotthold

Mattias.gotthold@datalawcenter.se

+46 (0)70 288 27 74

www.datalawcenter.se