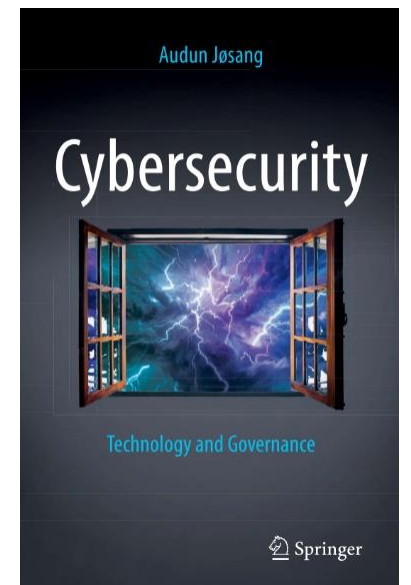


Chapter 10: Information Privacy

Cybersecurity: Technology and Governance

Audun Jøsang,

1st Edition, Springer Nature, 2024.



Overview

- Privacy and information privacy
- Online surveillance and tracking
- GDPR

Privacy and Information Privacy

- UN Universal Declaration of Human Rights – Article 12:
 - No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.
- European Convention on Human Rights - Article 8:
 - Everyone has the right to respect for his private and family life, his home and his correspondence.



Privacy

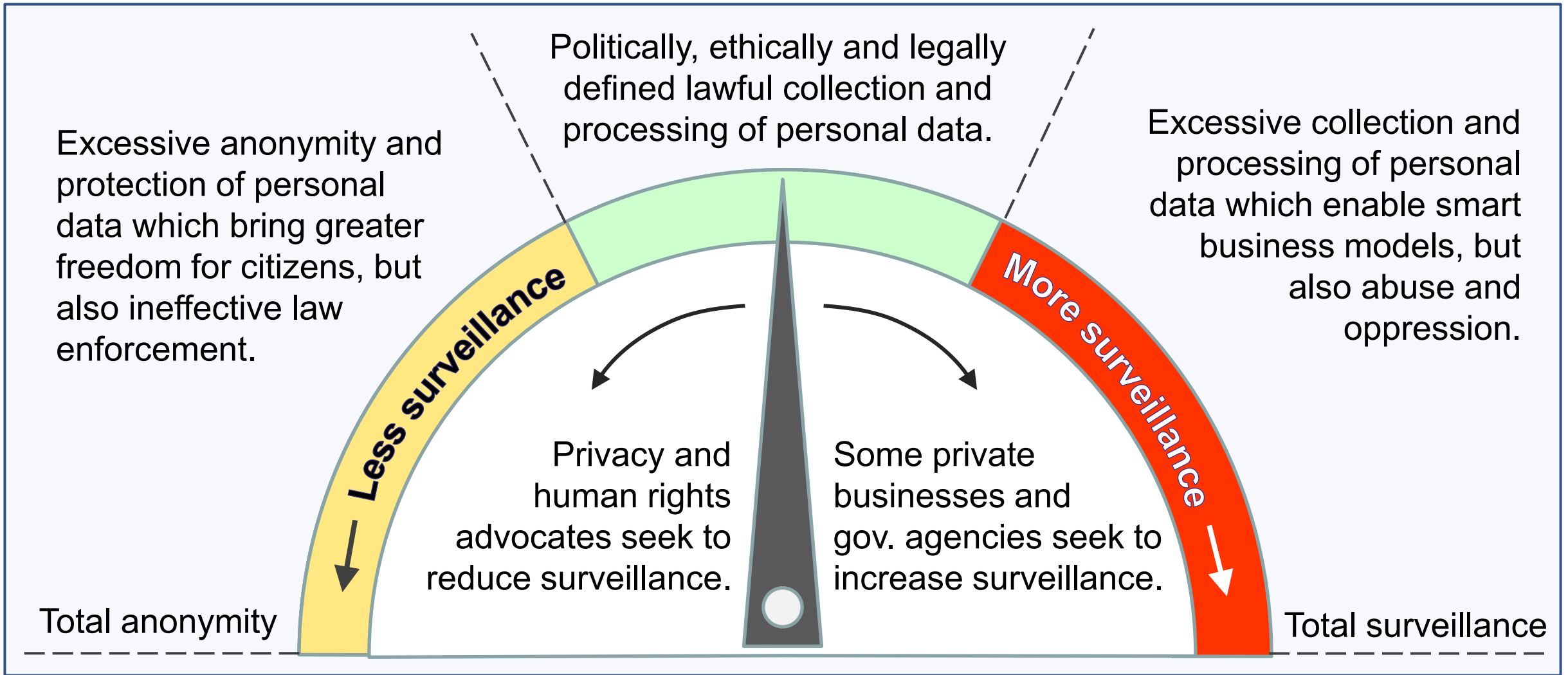


Information Privacy (Data Protection)



- “Data protection” is the EU jargon for “information privacy”

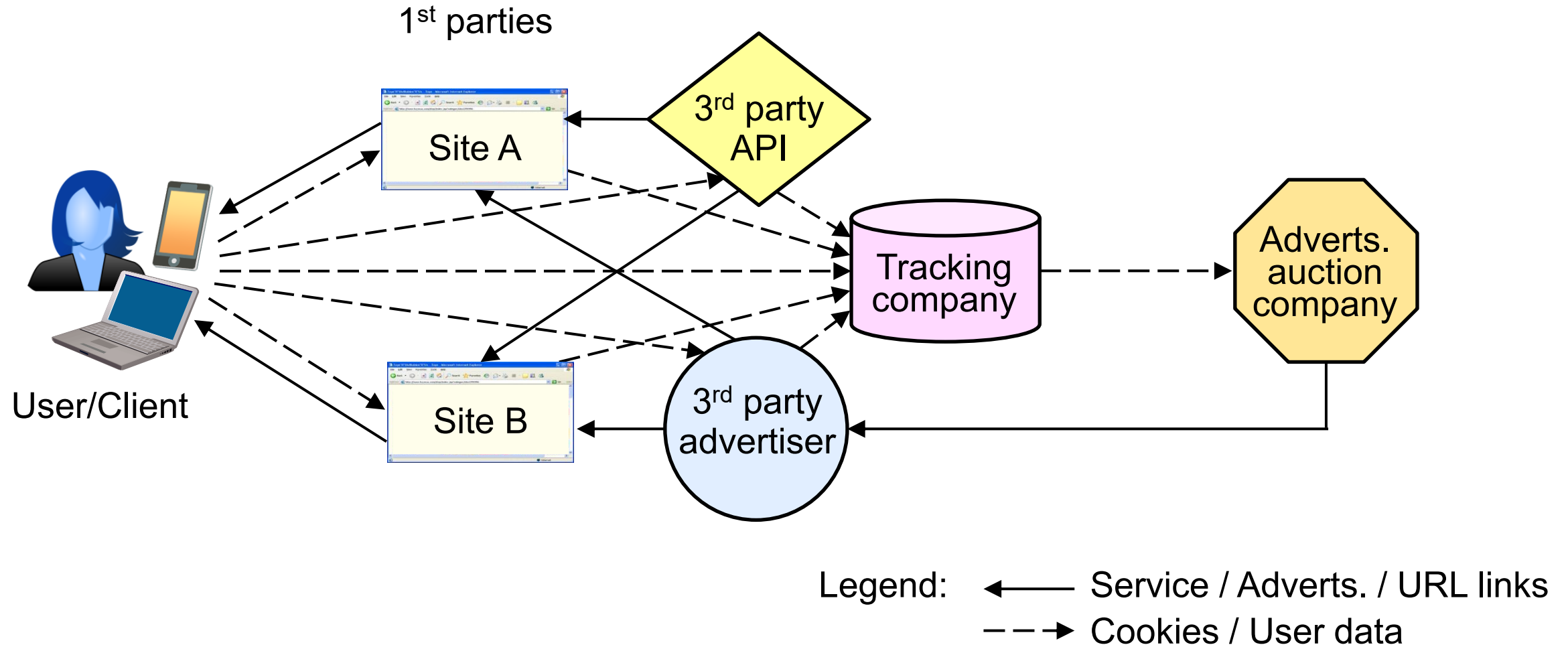
Surveillance barometer



Need for a balance between privacy and surveillance

- First, let's consider a state of massive collection of personal data
 - + It can support new business processes, streamline management, and make our lives easier
 - + Gives law enforcement agencies enormous opportunities to investigate crime and enforce law.
 - Will violate our integrity, create unwanted attention, cause our privacy to be exposed
 - Can lead to discrimination, abuse of power and oppression that can threaten our democracy.
- Let's then consider a state with minimal collection of personal data
 - + We can be left alone from unwanted attention from commercial companies
 - + We have less reason to fear abuse of power and repression by the authorities.
 - It will inhibit the development of smart business processes, make management inefficient
 - It will prevent effective investigation of crime. Giving disproportionately strong privacy to criminals and terrorists paralyzes law and order enforcement, which in turn can threaten our democracy.
- Conclusion: We need a good balance between privacy and surveillance

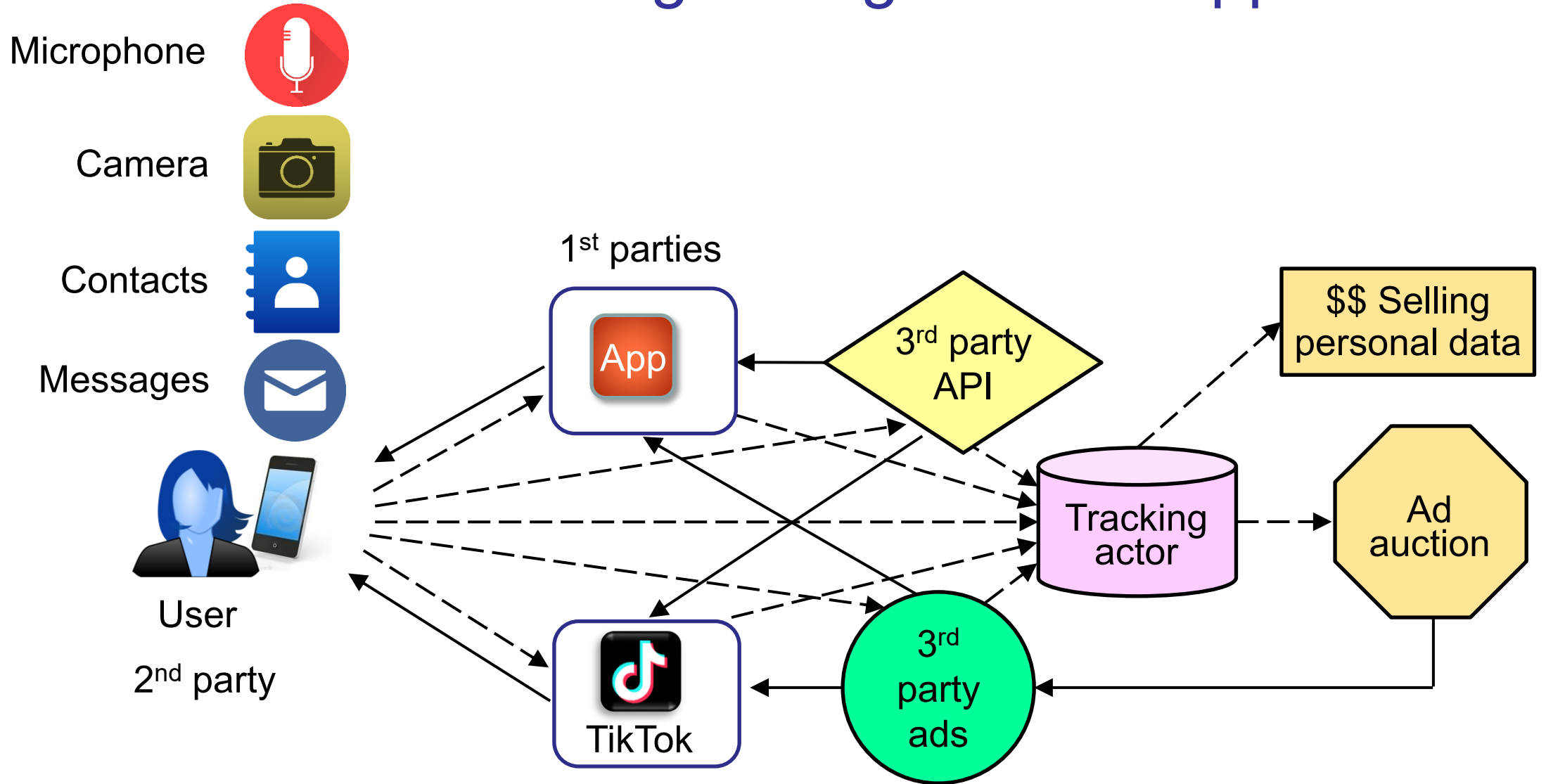
Tracking on the Internet



Ad auctions on the Internet

- Websites collect information about users over time, including cookies
- Additional features through third-party APIs also collect info in users.
- Tracking actors create profiles about users through data aggregation
- Websites that send a web page to the browser insert URL links to advertisements and other things that the browser itself loads from 3rd parties.
- The ad is selected by auctions that take place while the web page is loading
 1. The auction opens when advertisers receive a bid announcement for a web page that a user has clicked on. Advertisers receive the user profile so they can assess relevance.
 2. Advertisers each define their bid strategy based on how relevant the user is to them.
 3. In the end, the highest bidder advertiser wins the auction, automatically disseminating the advertisement that is integrated into the web page presented to the user, in the hope that the user sees and perhaps clicks on the advertisement.

Tracking through mobile apps



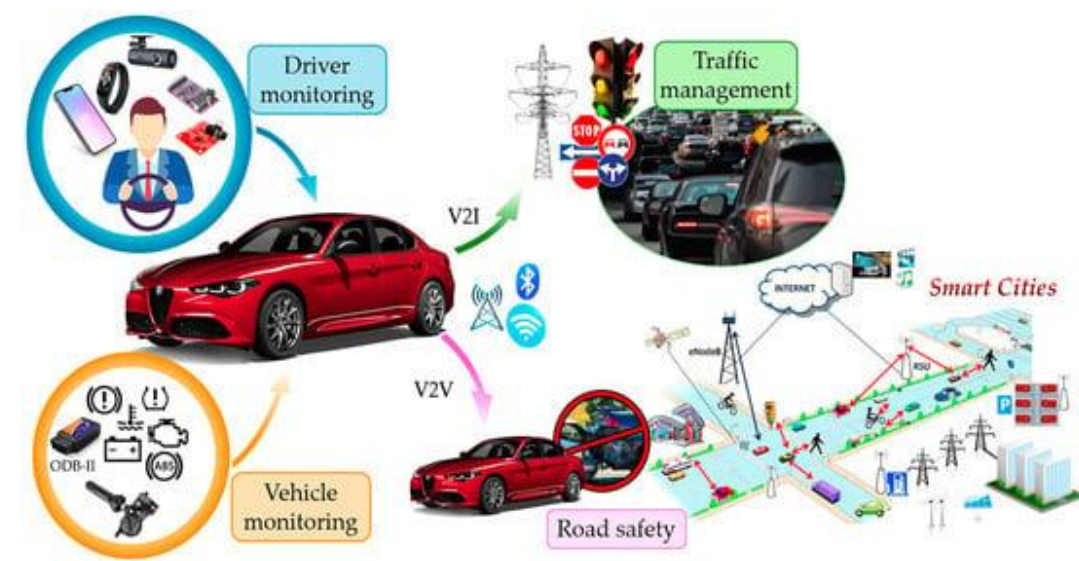
Apps that track and invade privacy

An orange rounded square icon with the word "App" in white text.

- Mobile apps usually require access to various resources on your mobile device, such as contacts, photos, microphone, camera, and location.
- We often consent to everything a mobile app asks for without much thought about it, because we want to start using the app as soon as possible.
- Technically, apps can...
 - activate camera and microphone at any time,
 - Send audio, video, messages, addresses, photos, and files to the app owner, e.g. to spy
- In 2023, many Western governments disallowed installing the apps TikTok and Telegram on mobile phones and other digital devices owned by public servants.
- TikTok and Telegram are like all other apps except that TikTok is Chinese-owned and Telegram is Russian-owned, and that China and Russia are considered threat actors.
- Chinese companies must hand over information that the authorities request.

Surveillance with cars

- Modern vehicles are packed with sensors.
- Is constantly online through the mobile network.
- Manufacturers update software.
- The vehicles send telemetry back to the manufacturer.
 - images, video, audio, continuous position, etc.
- Highly sensitive data in terms of security and privacy.
- Such data can lie unprotected and can be stolen by threat actors.
- Misconfiguration of Volkswagen's web platform leaked data from 800,000 electric cars across Europe, of which 80,000 are electric cars in Norway
 - <https://www.csoonline.com/article/3631055/volkswagen-massive-data-leak-caused-by-a-failure-to-secure-aws-credentials.html>
- State actors, e.g. China, can receive data from the manufacturers for espionage.



<https://doi.org/10.3390/s25020562>

EUR-Lex

 Experimental features ☐

Access to European Union law

EUROPA > EUR-Lex home > Regulation - 2016/679 - EN - gdpr - EUR-Lex

 Help  Print  Share

≡ MENU

 QUICK SEARCH



 Search tips

Need more search options? Use the [Advanced search](#)

Document 32016R0679

Text

Document information

Procedure

Document summary

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

OJ L 119, 4.5.2016, pp. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

 In force: This act has been changed. Current consolidated version: [04/05/2016](#)

ELI: <http://data.europa.eu/eli/reg/2016/679/oj>



Personal data, or PII (Personally Identifiable Information) is all information and assessments that can be linked to you as an individual.

The term "personal data" is equivalent to personal information.

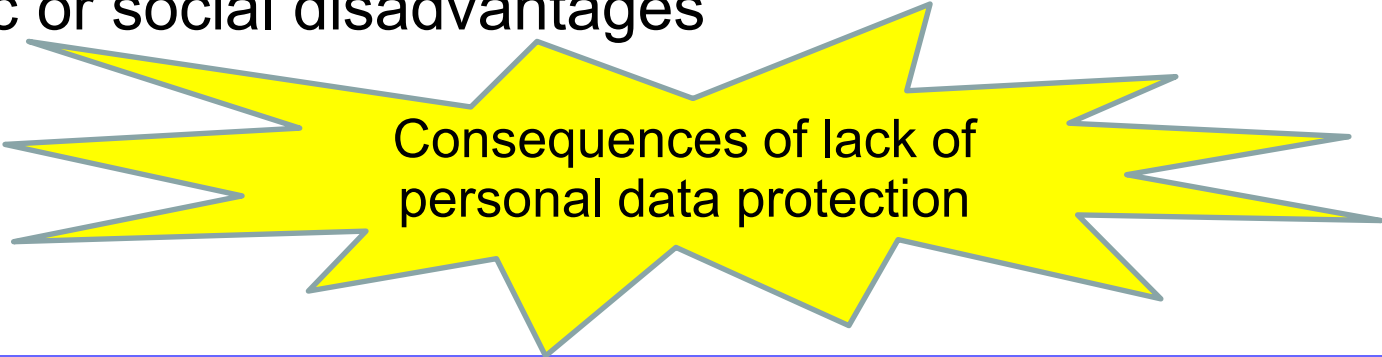
Data protection is to protect specific aspects of personal data:

- Prevent unlawful collection and retention of personal information
- Prevent unlawful use of collected personal information
- Ensure that personal information is correct
- Ensure openness and transparency
- Ensure adequate information security (CIA) around personal information
- Define clear responsibilities



Possible consequences of inadequate privacy

- Mental burden
- Unwanted attention
- Discrimination
- Identity theft or fraud
- Financial loss
- Damage to reputation
- Loss of confidentiality of confidential personal data
- Unauthorized revocation of pseudonymization
- Other economic or social disadvantages



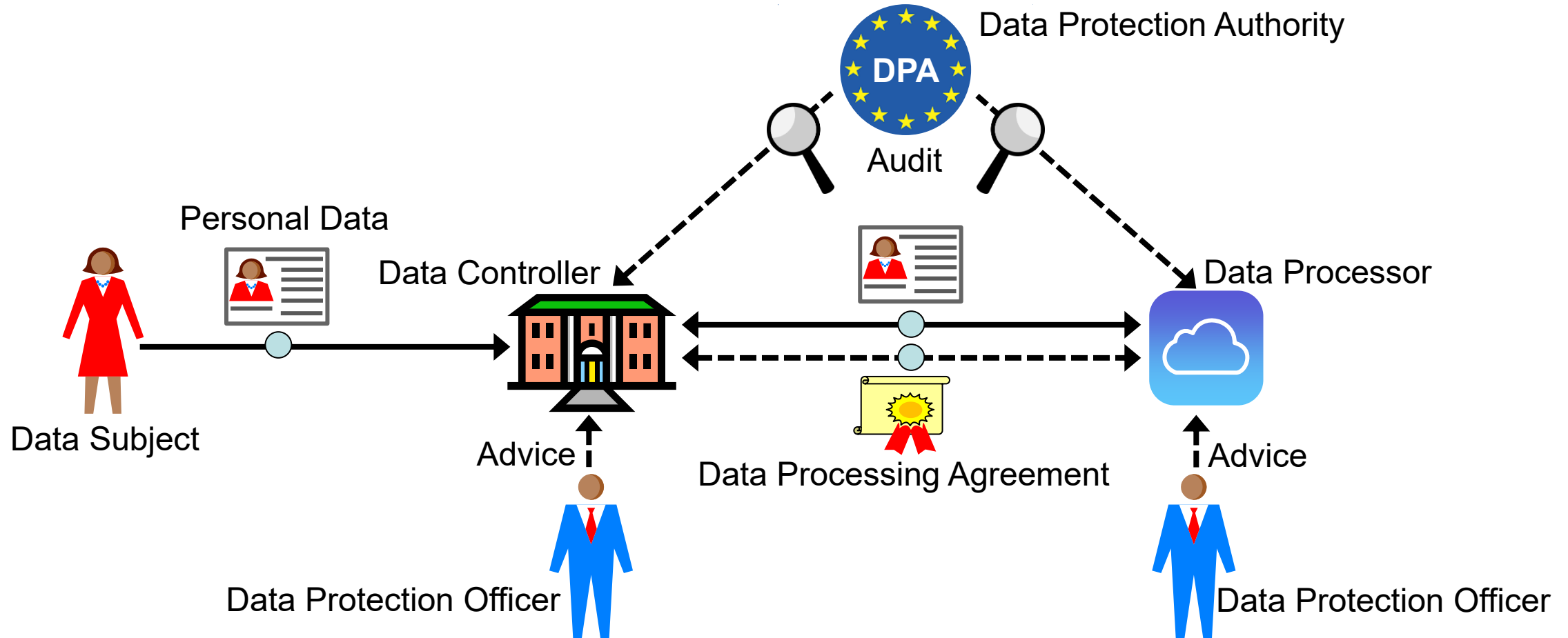
Consequences of lack of
personal data protection

General Data Protection Regulation (GDPR)



- Entered into force as law in the EU on 25.05.2018.
- Enforced by each country's data protection authority.
- The EU legal text (GDPR) is translated into every EU language, 99 articles .
- The following articles are presented here:
 - Art. 5: Principles relating to processing of personal data
 - Art. 6 and 9: Lawfulness (legal basis) of processing
 - Art. 25: Data protection by design and by default
 - Art. 32: Security of processing
 - Art. 35: Data protection impact assessment (DPIA)
 - Art. 45 and 46: Transfer of personal data to countries outside the EU/EEA
 - Art. 83: General conditions for imposing administrative fines

Roles in GDPR



Examples of personal data

Identity: Name, national identity number, marital status, height, weight, passport photo, fingerprints



Contact info: Home address, work address, mobile number, email address, username, etc.



Activity: Behavior patterns, interests, hobbies, studies, professional life, location, position, purchase patterns, search history, etc.



Communication: MAC and IP address, SMS, MMS, photographs, videos, social network, contacts, cookies etc.



Finance: Income, taxes, debts, bank account, bank statement, expenses, credit rating, etc.

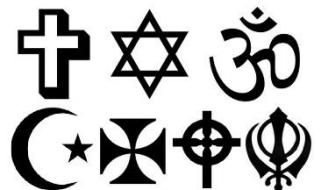


Pseudonymised information:

Woman, 43 years old, Oslo, likes to knit, has a sibirkat, works in public agency, two children.



Special categories: Health information, trade union membership, political opinion, religion, sexual relations/orientation, ethnicity/race



Art. 5: Principles relating to processing of personal data



1. *Personopplysninger skal behandles med:*
 - a) *Lawfulness, fairness, and transparency*
 - b) *Purpose limitation*
 - c) *Data minimisation*
 - d) *Accuracy*
 - e) *Storage limitation*
 - f) *Integrity and confidentiality*
2. *Accountability: The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').*

Art. 6: Lawfulness of processing



1. *Processing shall be lawful only if and to the extent that at least one of the following applies:*
 - a) *the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*
 - b) *processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
 - c) *processing is necessary for compliance with a legal obligation to which the controller is subject;*
 - d) *processing is necessary in order to protect the vital interests of the data subject or of another natural person;*
 - e) *processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
 - f) *processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

Point (f) shall not apply to processing carried out by public authorities in the performance of their tasks).

Art. 6.1.f: Legitimate interests of the data controller

- GDPR Art. 6(1)(f) may seem like a "blank cheque" for the processing of personal data, but it is not.
- To use Art. 6.1.f as a basis for processing, the controller must run a 3-point test, where the answer must be Yes to all 3:
 1. **Legitimate interest of processing:** Is there a legitimate interest behind the processing?
 2. **Necessity of processing:** Is the treatment necessary for that purpose?
 3. **Balance of interests:** Should the interests or fundamental rights and freedoms of the data subject prevail over the legitimate interests of the controller?
- Example of application of Art. 6.1.f: with the purpose of detecting insurance fraud:
 1. Indeed, insurance companies have a legitimate interest in preventing fraud.
 2. Indeed, the processing of specific personal data related to customers is necessary for this.
 3. The data subject's interest in not having personal data processed by insurance companies does not seem to outweigh the insurance companies' legitimate interest in preventing fraud.



Art. 6 and 9: Lawfulness of processing

Art. 9: Legal basis of processing special categories

- GDPR Article 9.1 points out that it is in principle prohibited to process special categories of personal data (see slide 16)
- GDPR Art. 9.2 defines exceptions that form the basis for processing for special categories.

Specification of legal basis of processing pursuant to Art. 6 and Art. 9

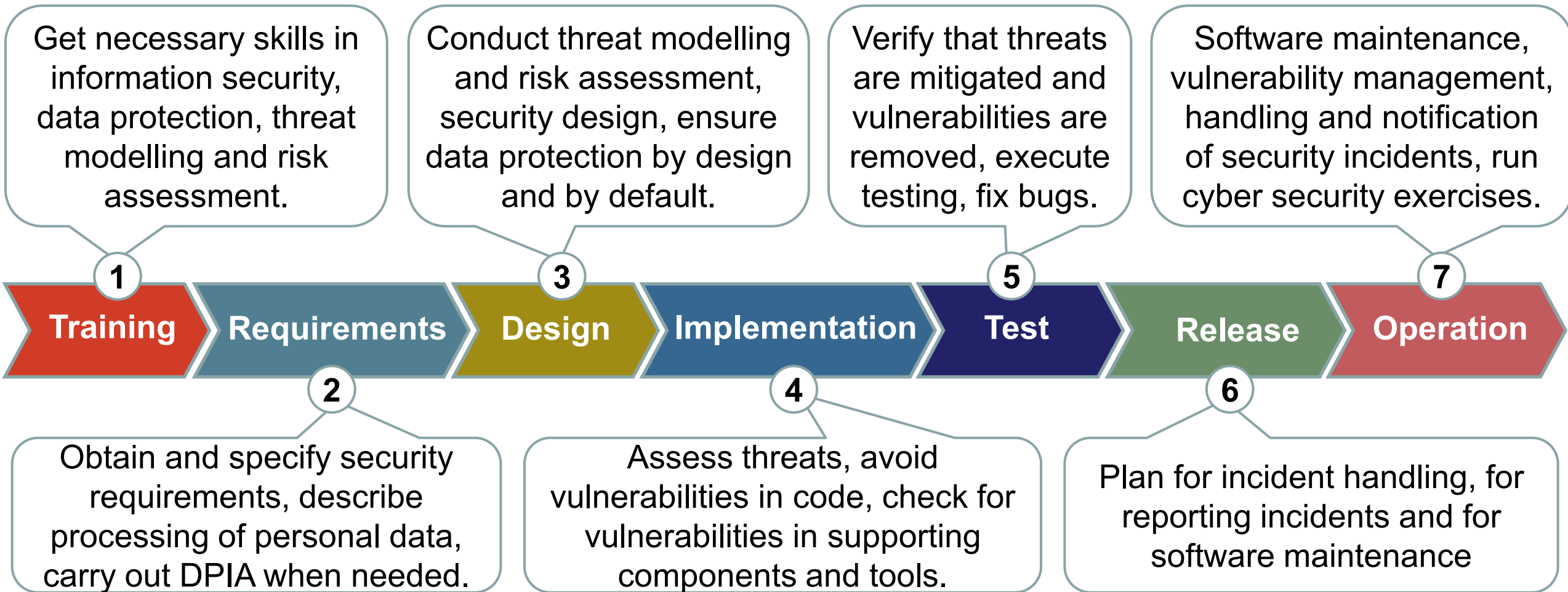
- For each type of personal data (e.g. name, address, e-mail, health information, membership of a political party, membership of a religious community), the data controller must be defined as a legal basis.
- Different types of personal data for the same processing may have different bases.
- Examples of legal bases:
- https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_en

Art. 25: Data protection by design and by default



- 1. Technical and organizational controls shall be implemented with a view to the effective implementation of the principles of protection of personal data, e.g. data minimisation, and to integrate the necessary safeguards into processing in order to comply with the requirements of this Regulation and to protect the rights of data subjects.*
- 2. The controller shall implement appropriate technical and organizational controls to ensure that, by default, only personal data necessary for each specific purpose of the processing is processed. That obligation applies to the amount of personal data collected, the scope of processing of the data, how long they are stored and their availability.*
- 3. An approved certification mechanism pursuant to Art. 42 Certification may be used as a factor to demonstrate compliance with the requirements laid down in paragraphs 1 and 2 of this Article.*

Privacy and information security by design



Guidelines from the Norwegian Data Protection Authority

<https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/data-protection-by-design-and-by-default/>

Art. 32: Security of processing



1. *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
 - a) *the pseudonymisation and encryption of personal data,*
 - b) *the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services,*
 - c) *the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident,*
 - d) *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*



Data Protection Officer



The Data Protection Officer advises data controllers or data processors on the company's obligations under the Data Protection Act. All companies can have a data protection officer.

A data protection officer must be appointed when:

- The processing is carried out by a public authority.
- The nature, scope and/or purpose of the data processing requires regular and systematic monitoring on a large scale.
- The main activity of the controller or processor consists of large-scale processing of special categories of data pursuant to Article 9 (sensitive personal data) or personal data related to criminal convictions and criminal offences referred to in Article 10.



Art. 45: Transfers on the basis of an adequacy decision

1. *A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation..*
2. *When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:*
 - a) *the rule of law, respect for human rights and fundamental freedoms, and relevant legislation*
 - b) *whether there are one or more well-functioning independent supervisory authorities in the 3rd State*
 - c) *international commitments the 3rd country or international organisation concerned has entered into*
3. *The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article (adequacy decision).*

Countries covered by an adequacy decision



- An adequacy decision for a state or territory means that the transfer will be comparable to transfers between countries within the EEA.
 - Eliminates the need to define other bases of transfer of personal data.
- As of 2025, adequacy decisions apply to the following countries:

Andorra	Argentina	Guernsey	Isle of Man
Israel	Jersey	New Zealand	Sveits
Storbritannia	Uruguay		
- Under certain conditions, the adequacy decision also applies to the following countries:

Canada	Færøerne	Japan	Sør-Korea
USA			
- See info from the EU Commission:
 - https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

The Schrems-II verdict



- Max Schrems argued that the adequacy decision for the US based on the Privacy Shield agreement was a violation of the GDPR, due to the following laws:
 - FISA Section 702 (Foreign Intelligence Surveillance Act) allows for the collection of intelligence on non-US persons who are not located in the United States.
 - Executive Order 12333 governs all U.S. foreign intelligence activities, including activities that fall outside FISA, such as those conducted abroad against non-U.S. persons. Intelligence activities can take place secretly.
 - Presidential Policy Directive 28 allows for the mass collection of (personal) data for surveillance without affected persons being specifically suspected or designated as of interest. However, the data obtained can only be used for national security, and not, for example, for industrial espionage
- On 16.07.2020, Max Schrems won the case, and the Privacy Shield was repealed.
- After the judgment, transfer to the USA had to be based on Art.46 and Art.47.
- On 10.07.2023, the new EU – US Data Privacy Framework was established
 - Again, an adequacy decision has been made for transfer to the USA for U.S. businesses certified under this agreement. Max Schrems has announced plans to challenge the new agreement.

Art. 46: Transfers subject to appropriate safeguards



1. *In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.*
- Processing in non-EU/EEA countries that lack an adequacy decision, must be assessed in the light of GDPR Art. 46. Elements that need to be considered include:
 - Sensitivity level of the personal data.
 - Encryption and anonymization can be a solution for IaaS and PaaS, but is impractical when using SaaS. Encryption keys stored in 3rd countries do not provide any protection, because their governments may require them to be handed over. Admin access from the 3rd countries means transfer out of the EU/EEA even if data is stored in the EU/EEA.

Art. 83: General conditions for imposing administrative fines



1. *Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of the GDPR.*
2. *When deciding whether to impose an administrative fine and deciding on the amount of the fine in each individual case due regard shall be given to e.g.:*
 - a) *the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected, and the level of damage suffered by them;*
 - b) *the intentional or negligent character of the infringement.*
4. *In the case of minor infringements, fines of up to €10,000,000 or, in the case of an enterprise, of up to 2% of the total global annual turnover in the preceding financial year, where the highest amount is applied, may be imposed.*
5. *In the case of serious infringements, fines of up to €20,000,000 or, in the case of an enterprise, of up to 4% of the total global annual turnover in the preceding financial year, may be imposed, whichever is higher:*

DPIA

Data Protection Impact Assessment



Hens
(personal data)

The fox
(the organization)

The organization gets a conflict of interest when performing DPIA.
It is analogous to *"letting the fox guard the hen house"*.

Art. 35: Data protection impact assessment (DPIA)



1. *Where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (conduct a DPIA).*
2. *The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.*
3. *A DPIA shall in particular be required in the case of:*
 - a. *a systematic and extensive evaluation of personal aspects relating to natural persons,*
 - b. *processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences,*
 - c. *a systematic monitoring of a publicly accessible area on a large scale.*

What is meant by "**rights and freedoms**" is first and foremost the rights described in GDPR Articles 12 – 22, but also rights enshrined in the UN Human Rights and the European Convention on Human Rights, which among other things describe the right to privacy, protection of communication, freedom of expression, freedom of religion, the right to organize, and freedom from discrimination.

Two types of privacy risks

Depending on who the threat actor is



Threat actors:

- script kids
- hacktivism
- Organised crime
- terrorism
- Government cyber operations



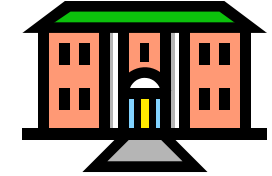
Threats include:

- CIA Personal Data Breach
- Theft and publication of personal data

→ Risk assessment according to Art. 32.

Threat actors:

- the data controller
- the data processor



Threats include:

- Unwanted collection
- Unfair discrimination
- Re-identification
- storage longer than necessary

→ DPIA according to Art. 35.

DPIA creates a conflict of interest analogous to *“letting the fox guard the hen house”*.

Cybersecurity risk assessment is not DPIA!

- Art.32 relates risk assessment to the personal data security of the processing (not DPIA)
 - carried out before treatments, updated regularly and in the event of changes
 - identify areas that may result in accidental or unauthorized access, alteration, deletion, loss or disclosure of personal data;
 - will acquire knowledge about the risks that exist
 - is necessary to be able to implement adequate security measures
- Art.35 relates risk assessment to privacy impact (DPIA)
 - are carried out for processing activities that are likely to entail a high risk to rights and freedoms;
 - The purpose is to manage a risk in invasive treatments that entail an increased risk of violating the rights and freedoms of natural persons. Security measures will not necessarily reduce this risk, and risk-reducing measures must focus on how the treatment is carried out and how rights are safeguarded.

When is DPIA mandatory?

*«Where a type of processing in particular using **new technologies**, and taking into account the **nature, scope, context** and **purposes** of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.»*
(Art. 35.1)

- The assessment is mandatory when the treatment is likely to involve a high risk. If it is uncertain whether it is necessary to carry out a DPIA, it is recommended to do so anyway, as a useful tool for the data controller to be sure that they comply with the GDPR.

Nature

Intrinsic characteristics of the processing:

- Difficult to exercise one's rights
- Unpredictability, little transparency and uncertainty about safeguarding principles
- Systematic treatment
- Special categories
- Skewed power balance
- New technology

Scope

The scope of the processing:

- Number of subjects involved (figures or %)
- Data volume (number of variables, details)
- Storage time (short, temporary, permanent)
- Geographical scope (local, regional, national, international, global)

Purposes

What will the personal data be used for:

- Control purposes
- Processing for the purpose of making decisions that affect the data subject
- For decisions about individuals based on systematic and comprehensive analysis of personal data

Context

What expectation of privacy surrounds it

Specific treatment:

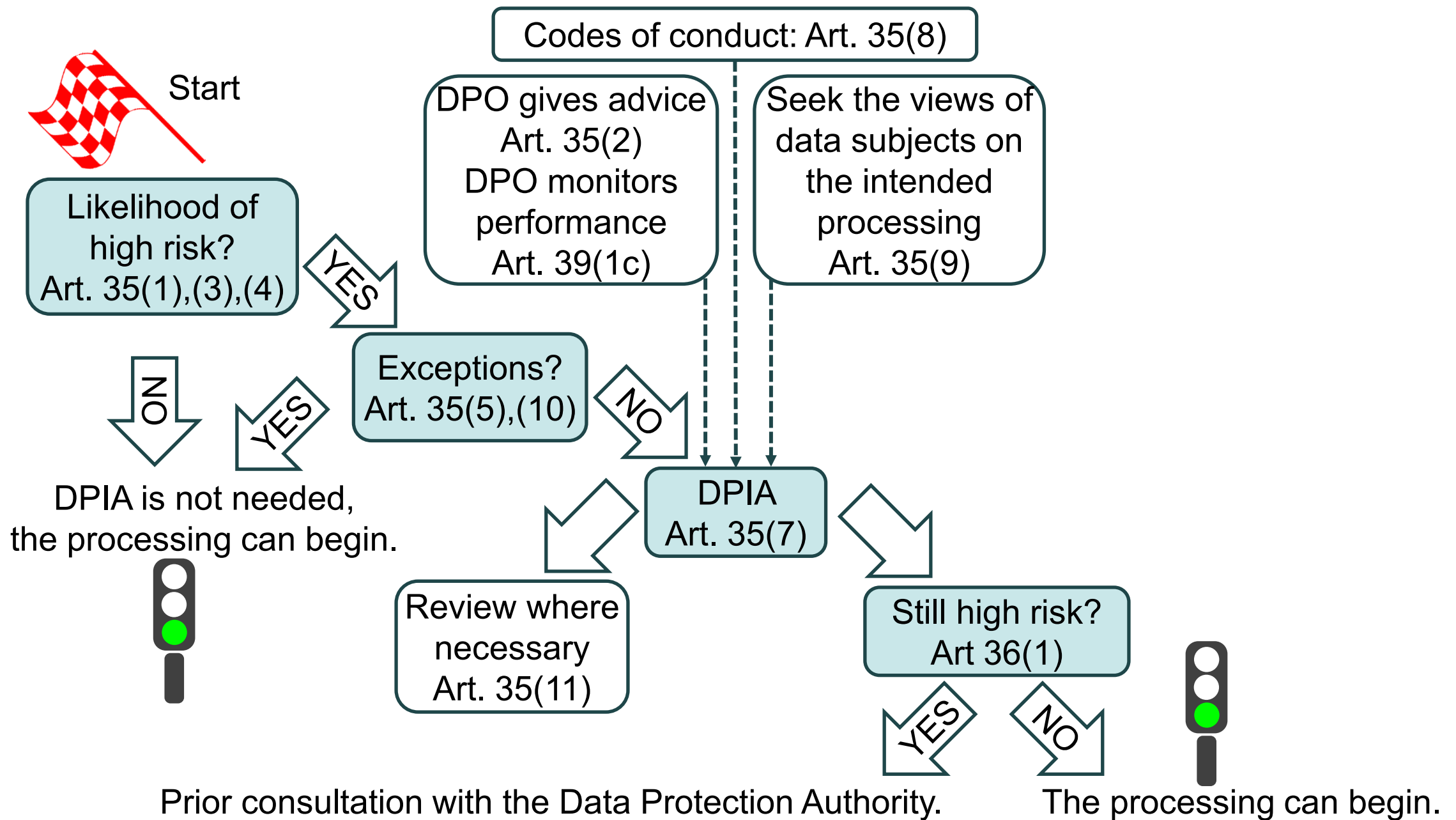
- Expectation of confidentiality (health, welfare, working conditions)
- Expectation of privacy (home, recreation)
- Processing of data from different data sets collected for different circumstances

Absolute necessity of DPIA



- DPIA is absolutely necessary in the following cases:
 - systematic and comprehensive assessment of personal circumstances when the data is used for automated decision-making
 - processing of special categories of personal data on a large scale;
 - Systematic monitoring of public areas on a large scale
- The Data Protection Authority **must** publish a list of when it is required
- The Data Protection Authority **may** publish a list of when it is not required

Art. 35 (3-5)



Participants in conducting a DPIA

- The data controller:
 - The work itself can be delegated to others, but the data controller is accountable for the lawfulness of the processing
- Participants
 - Data processors
 - The Data Controller must obtain the views of the data subjects or their representatives, if this is relevant
 - Good practice: involving relevant actors and, where appropriate, experts in the field
 - The CISO and PVO can recommend that a DPIA be carried out, and contribute to the process
 - The data protection officer often prefers not to participate in the DPIA because it creates a conflict of interest.



DPIA Planning

- Prerequisite: The processing must be lawful and meet the basic requirements that follow from the other provisions of the Regulation
 - A DPIA must be carried out prior to treatment, and should be started as early as possible.
 - It is a continuous process, not a one-time occurrence.
- Follow good practices:
 - Define and document roles and responsibilities.
 - Document why you may be conducting a processing that is contrary to the views of the data subjects.
 - Document why you may not ask for the data subject's views at all.



Key Elements of DPIA



Steps in the DPIA process:

1. «Prepare a systematic description of the planned treatment and the purpose of the treatment»,
2. "Make an assessment of whether the processing activities are necessary and proportionate to the purposes",
3. "Carry out an assessment of the risks to the rights and freedoms of the data subjects",
4. "Specify the planned controls and measures":
 - "to manage the risks",
 - "to demonstrate compliance with the GDPR".
5. Get management validation of the DPIA.

In practice, the DPIA team will first draft a systematic description, then make an iteration over points 1 – 4 until it is assessed that "processing will not have consequences for the rights and freedoms of the data subject", and finally edit the final version of the systematic description, which is validated by management.

Art. 35 (7)

Systematic description of the processing



- Review and quality-check overview and description of the processing
 - The nature, scope, purpose and context of the processing
 - Recipients, data flow and storage
 - Functional description of the treatment and all assets
 - Relevant references for the treatment are documented.
- **Goal:** The data controller has a complete overview of the processing, and does a quality check to ensure that the descriptions made are complete and clear.

Art. 35 (7.a)

Necessity and proportionality

- Basis for processing
- Transfer basis
- Purpose(s)
- Data minimization
- Correctness
- Storage limitation
- Rights of data subjects
- Freedoms of data subjects

Check whether it is necessary or possible to improve the way in which the privacy principles are safeguarded, and the rights and freedoms of data subjects. Where possible, review the description again or suggest additional actions.

Goal: In this phase, quality assurance is ensured that the choices are legitimate and carried out to help ensure that the processing is necessary and proportionate to the purpose, in order to comply with legal requirements



Art. 35 (7.b)

Assessment of consequences and planned measures

- Assessment of the risk of violation of rights and freedoms
 - Lack of necessity and proportionality
 - Lack of real co-determination
 - Lack of real transparency
 - Lack of predictability
1. Identify threats
 2. Clarify potential consequences
 3. Estimate the likelihood of an event occurring
 4. Estimate the severity of each risk
 5. Determine measures to manage the risks
- **Goal:** Have a processing that does not have consequences for the rights and freedoms of the data subject.



Art. 35 (7.c-d)

How to assess privacy impact?

- Assess the likelihood and consequence of that (non-exhaustive list!):
 - Personal data is processed without a legal basis
 - Personal data is processed in an unfair manner
 - There is a lack of transparency regarding the processing of personal data
 - More personal data is collected than necessary for the purpose
 - Personal data that is processed is not correct
 - personal data is stored longer than necessary for the purpose
 - the data subject lacks the information to make an informed choice
 - the data subject does not have access to stored personal data
 - the data subject does not have their personal data corrected or deleted
 - data portability has not been facilitated
 - the rights of the data subjects are not safeguarded by profiling
 - The treatment may result in discrimination
 - The processing restricts freedom of expression and freedom of religion

Examples of privacy controls and measures

- Collect less personal information
- Reduced processing of personal information
- Permitted right of reservation
- Ongoing information, multiple channels
- Specially adapted access portal
- Automatic deletion
- Anonymization
- Explainable AI
- Alternative manual procedure for decision



Management validation of the DPIA

- Prerequisites that management **MUST** be aware of:
 - The enterprise has a processing that is likely to entail a high risk to the rights and freedoms of the data subjects, and is covered by Article 35.
 - Must gain an understanding of the completed DPIA, identified risks and measures.
 - Failure to do the DPIA, performing the DPIA incorrectly, or not consulting with the correct authorities may result in administrative fines
- Prepare documentation for management validation:
 - Compile and present findings
 - Document the consideration of stakeholders
 - Management review, decision, and approval



Management's decision on DPIA

- The management decides and justifies whether the DPIA is:
 - Approved/validated => Processing can start.
 - Conditional on improvements (explain in what way) => Revised DPIA must be presented again to management.
 - Rejected: The enterprise decides not to carry out the processing.
 - When the DPIA is:
 - in the management team more than once, and
 - The risk is still high and the willingness to process data is still high
- => Necessary to request a prior discussion with the Data Protection Authority.
- The organization must document that the risk cannot be reduced.
 - The decision to request a preliminary discussion shall be made by the management.



Prior consultation with the Data Protection Authority

- In the event of high risk, which cannot be reduced, the Data Protection Authority shall be involved in prior discussions.
- There are requirements for documentation to be submitted, and that the data controller has followed the Data Protection Authority's guidance.
- The maximum processing time at the Data Protection Authority is 8 (+ 6) weeks.
- A written, formalised process that will assess:
 - whether the processing takes place in accordance with the GDPR, safeguards the privacy principles, the rights and freedoms of the data subjects
 - whether the controller has sufficiently identified the risk
 - whether the risk has been sufficiently reduced
- **Goal:** Avoid processing of personal data that entails a high risk to the rights and freedoms of the data subjects

References

Guidelines:

- Conducting a DPIA:

<https://gdpr.eu/data-protection-impact-assessment-template/>

- Software development with privacy by design:

<https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/data-protection-by-design-and-by-default/>

End of presentation
