CONSIDERATI

INTRODUCTION OF THE DATA PROTECTION REFORM TO THE JUDICIAL SYSTEM
INFORM

Legitimate processing & supervision

INFORM DAY

Mr. dr. Bart W. Schermer
Chief Knowledge Officer
schermer@considerati.com

Principles of the fairness of processing (art. 5 GDPR)

a) Processed lawfully, fairly and in a transparent manner (…) **(lawfulness, fairness and transparency)**

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (…) **(purpose limitation)**

c) adequate, relevant and limited to what is necessary (…) **(data minimisation)**

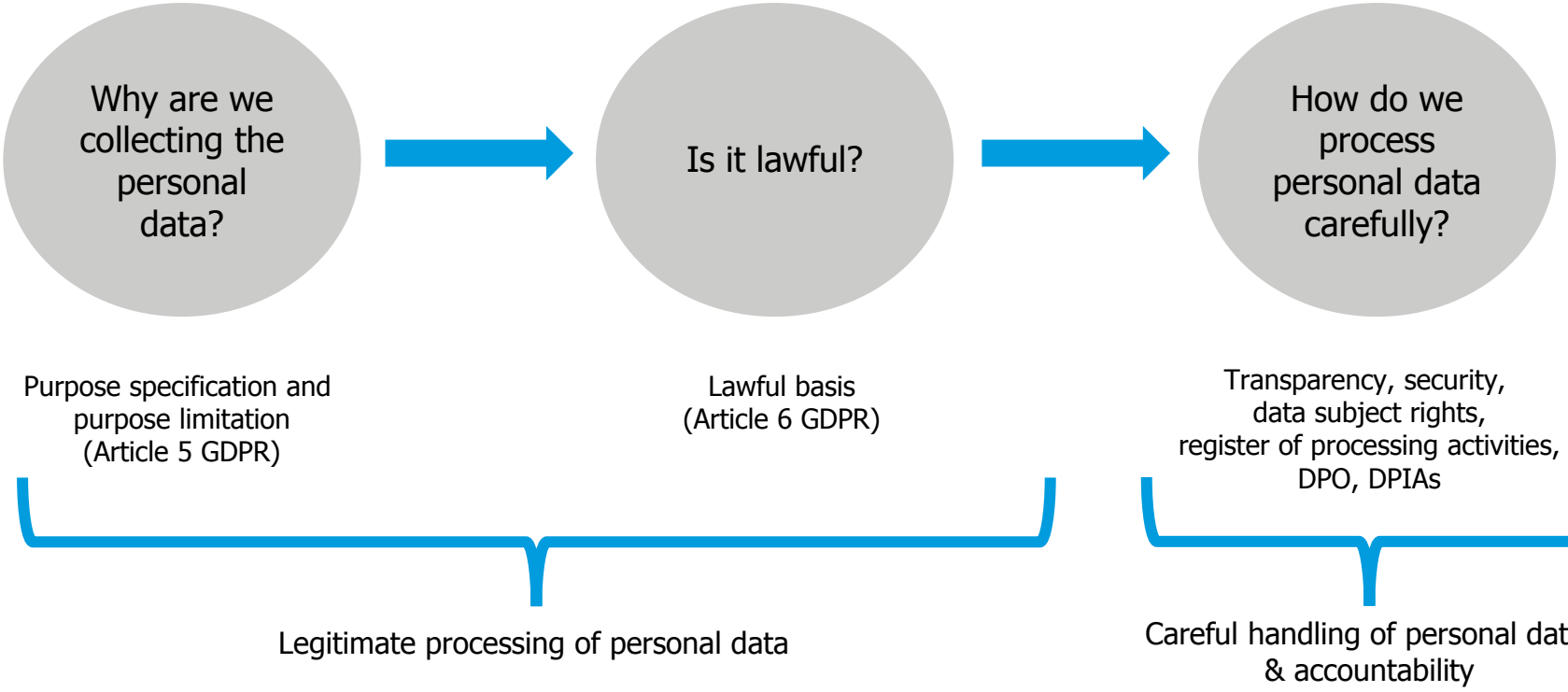
d) accurate and, where necessary, kept up to date (…) **(accuracy)**

e) kept in a form which permits identification of data subjects for no longer than is necessary (…) **(storage limitation)**

f) processed in a manner that ensures appropriate security of the personal data (…) (**integrity and confidentiality**)

What does the GDPR say?

The GDPR mandates the lawful and proper processing of personal data



Legitimate processing

- Personal data may only be collected for a specified purpose
- That purpose must be legitimized (based in a lawful basis from the GDPR)
- The legal bases are:
  a) Unambiguous consent
  b) Necessary for the performance of a contract
  c) Necessary for the compliance with a legal obligation
  d) Necessary in order to protect the vital interests of the data subject
  e) 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) Necessary for the purposes of the legitimate interests pursued by the controller

Unambiguous consent

Article 4 (11) GDPR

'consent' of the data subject means any **freely given**, **specific**, **informed** and **unambiguous** indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Obtaining consent in practice

"I agree to the general conditions"

Versus

"I agree to the privacy policy"

Versus

"I agree with the processing of my personal data to receive personalized offers"

NB= pre-ticked boxes will not be accepted as unambiguous consent by the supervisory authority!

Pop-Quiz

Determine the lawful basis for which personal data can be processed in the following situations

- … a lawyer processes the contact details of a client for invoicing purposes.
- … a lawyer uses cookies to identify the online surfing behavior of potential clients and uses that to send them targeted offers and/or advertisements for legal services.
- … the Court of Amsterdam sends salary data of its employees to the Dutch Tax Authority.
- … the Court of Amsterdam installs security cameras to monitor and guard its business premises en installations.
- …the Public prosecutor sends dossiers of suspects to the court of Amsterdam for trial

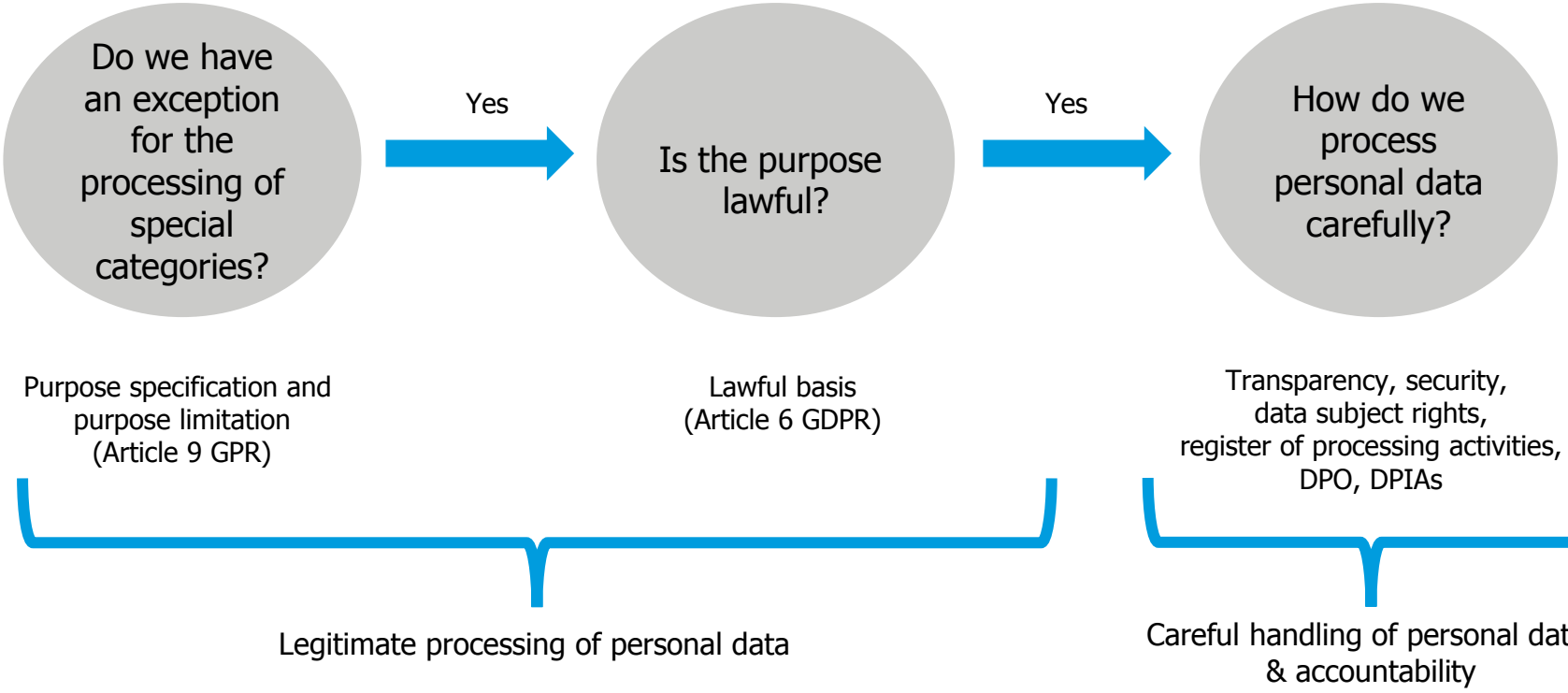
Specific exemptions for courts

"While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities."

Special categories of personal data

Special categories of personal data (art. 9)	Other highly sensitive data
Racial or ethnic origin	Personal data relating to criminal convictions and offenses (article 10 GDPR)
Political opinions	National identification numbers (87)
Religious or philosophical beliefs	
Trade union membership	
Genetic data	
Biometric data for the purpose of uniquely identifying a natural person	
Data concerning health	
Data concerning a natural person's sex life or sexual orientation	

Use of special categories of data



Exemptions for special categories of data

- Article 9 + article 10
- National implementing acts provide specific rules for use of special categories of data
- *"A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure." (recital 52)*
- *Article 9(f): processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;*

Exemptions for special categories of data

Example from Dutch implementing act (Uitvoeringswet AVG)

Artikel 22e (algemene uitzonderingen verwerking bijzondere persoonsgegevens):

de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering, of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid.

Artikel 32d (strafrechtelijke gegevens):

de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering, of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid;

Supervision

Internal and external supervision

Supervision

What kinds of supervision are there?

- Internal supervision
- External supervision

Internal supervision

Relevant roles and people

- Board
- Management
- DPO
  - Privacy coordinators
- Compliance / Legal

Data Protection Officer

The DPO

Article 37

Data protection officer

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

a) the processing is carried out by a public authority or body, **except for courts acting in their judicial capacity**;

b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

Data Protection Officer

The DPO

Article 39

Tasks of the data protection officer

The data protection officer shall have at least the following tasks:

b) To monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

c) To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 55;

d) To cooperate with the supervisory authority {…}.

External supervision: Supervisory Authorities

National supervisory authorities & European Data Protection Board

The supervisory authority under the GDPR

Article 51 GDPR

- One or more supervisory authorities per Member State

- Independence

Specific exemptions for courts

Recital 20

*"**The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary** in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations."*

Specific exemptions for courts

Example: Dutch situation

"1. Het toezicht op de verwerking van persoonsgegevens door gerechten en het parket bij de Hoge Raad in het kader van de uitoefening van hun gerechtelijke taken wordt toevertrouwd aan de door de gerechten en het parket bij de Hoge Raad aangewezen functionarissen voor gegevensbescherming (verder: FG's) en aan de procureur-generaal bij de Hoge Raad."

*Regeling toezicht verwerking persoonsgegevens door gerechten en het parket bij de Hoge Raad

Tasks of the supervisory authority (I)

Article 57 GDPR

a. Monitor and enforce the application of this Regulation
b. Promote public awareness and understanding with the general public
c. Advise the national parliament, government, etc.
d. Promote the awareness of controllers and processors of their obligations
e. Upon request, provide information to data subjects (concerning the exercise of their rights)
f. Handle complaints lodged by data subjects
g. Cooperate with other supervisory authorities with a view of ensuring the consistency of the application and enforcement of the Regulation

Tasks of the supervisory authority (II)

Article 57 GDPR

h. Conduct investigations
i. Monitor relevant developments that impact the protection of personal data (m.n. IT)
j. Adopt standard contractual clauses for transfers
k. Establish and maintain a list of DPIA-required processing activities
l. Give advice in response to prior consultation
m. Encourage the drawing up of codes of conduct
n. Encourage the establishment of data protection certification mechanisms/seals
o. Carry out periodic review of certifications
p. Draft and publish the criteria for accreditation of a body for monitoring codes of conduct and certifications

Tasks of the supervisory authority (III)

Article 57 GDPR

q. Accredit bodies responsible for monitoring codes of conduct and certifications
r. Authorize contractual clauses and provisions for transfers
s. Approve BCRs
t. Contribute to the activities of the EDPB
u. Maintain internal records of infringements and corrective measures taken
v. Fulfil any other tasks related to the protection of personal data

Powers of the supervisory authority (I)

Article 58 GDPR – Investigative powers

- Order organizations to provide any information required for the performance of its tasks
- Carry out investigations in the form of data protection audits
- Carry out reviews on issued certifications
- Notify organizations of alleged infringements
- Obtain access to all personal data and all information necessary for the performance of its tasks
- Obtain access to any premises (including any data processing equipment and means)

Powers of the supervisory authority (II)

Article 58 GDPR – Corrective measures

- Issue warnings to organizations where their intended processing are likely to infringe the Regulation
- Issue reprimands to organizations where their processing has infringed the Regulation
- Order organizations to comply with data subject requests
- Order organizations to bring their processing into compliance with the Regulation
- Order organizations to communicate a personal data breach to data subjects
- Impose a temporary or definitive limitation including ban on processing
- Order the facilitation of data subject rights
- Revoke a certification
- Impose an administrative fine
- Order the suspension of data flows

Powers of the supervisory authority (III)

Article 58 GDPR - Authorization and advisory powers

- Provide advice in accordance with the prior consultation procedure after a DPIA
- Issue advice on its own initiative (or upon request)
- Authorize processing after the prior consultation procedure
- Approve draft codes of conduct
- Accredit certification bodies
- Issue certifications and approve criteria of certification
- Adopt standard contractual clauses
- Authorize administrative arrangements, contractual clauses, and BCRs.

Power to impose fines (I)

Considerations for the imposition of an administrative fine

- Effective, proportionate, and dissuasive

- Amount of the fine is partially dependent on, among others:
  - Nature, severity and length of the infringement
  - Intentional or negligent nature of the infringement
  - (Mitigating) measures taken

Power to impose fines (II)

Amount of the fine

- 10.000.000 EUR or 2% global annual turnover
  - Obligations on organizations

- 20.000.000 EUR or 4% global annual turnover
  - Principles, legal bases, data subject rights and transfers

Pop-Quiz

Case study

It has been known for several months that your organisation's HR software has a bug. Due to a recent restructuring, there is nobody within your organization who is currently responsible for resolving the issue. Last week, something finally happened that you (as DPO) were afraid of… The company HR system has been compromised and personal data is been hacked and leaked outside to unauthorized parties.

As DPO, you are asked to make an assessment of the risk faced by the company of an administrative fine laid down by the Dutch Data Protection Authority (Autoriteit Persoonsgevens).

Layered System of European Supervision

From national to European

National supervisory authority competent within their own territory

Appoint lead supervisory authority with cross-border processing

Cooperation between lead and involved supervisory authorities aiming to achieve consensus

When needed, dispute resolution through the consistency mechanism by the EDPB

Definitive decision made against organization by lead supervisory authority

Competent on own territory

National supervisory authority on own territory

- Every supervisory authority is competent on their own territory to:
  - Carry out their tasks; and
  - Exercise their powers.

- If a case only concerns an establishment in a Member State or data subjects within that Member State are affected, the supervisory authority is also competent.
  - Notify the lead supervisory authority.

Cross-border processing

National supervisory authority on own territory

There is an instance of cross-border processing where:

a) The processing of personal data takes place in the context of activities of establishments in more than one Member State of a controller or processor in the Union established in one or more Member State; or

b) The processing of personal data takes place in the context of activities of an establishment of a controller or processor in the Union, but where data subjects of more than one Member State are significantly affected or likely to be significantly affected.

Lead supervisory authority (I)

Main establishment is decisive for determining the lead supervisory authority

- Main establishment of an organization is important for determining the lead supervisory authority.
- Criteria for determining the main establishment (Guidelines WP29):
  - Central administration / headquarters
  - Where are the decisions made about the purposes and means?
  - Where are the decisions taken about the business activities where personal data are processed?
  - Where does the authority lay to implement the decisions?
  - Where is the CEO / Board situated?
  - Where is the controller or processor registered in the Chamber of Commerce?

Lead supervisory authority (II)

In cross-border situations

- The lead supervisory authority is competent with respect to the controller or processor concerned

- The lead supervisory authority is the only contact point for the controller or processor in cross-border processing situations.

- Eventual decision-making authority by the lead supervisory authority

- Cooperate with other involved supervisory authorities to try and reach a consensus

Lead supervisory authority (III)

Exemptions to the powers of the lead supervisory authority

- The supervisory authority is also competent where a case only concerns an establishment in that Member State or only significantly affects data subjects in that Member State, despite the fact that another supervisory authority is the lead.

- Notify the lead supervisory authority who can still decide to handle the case themselves.

Involved supervisory authority

When is a supervisory authority involved?

- An involved supervisory authority is an supervisory authority who is involved with the processing of personal data because:
  - The controller or processor is established (also) on their territory;
  - Data subjects in that Member State are significantly affected (or likely to be) by the processing;
  - A complaint is lodged with that supervisory authority.

Cooperation (I)

Cooperation between the lead supervisory authority and the other supervisory authorities

- Leading supervisory authority shall make a draft decision and submit it to the other involved supervisory authorities

- Relevant and reasoned objection to be made within 4 weeks

- If the leading supervisory authority does not follow the objection, the matter with be submitted to the consistency mechanism

- The final decision is made by the lead supervisory authority

Cooperation (II)

Practical realization

- Mutual assistance; exchanging information and cooperating in investigations.

- Joint operations; joint teams of members from the lead and involved supervisory authorities.

European Data Protection Board

EDPB

- Legal personhood
- Heads of one supervisory authority per Member State
- The Chair and two vice-Chairs will be chosen among them
- The Secretariat is fulfilled by the European Data Protection Supervisor

Consistency mechanism

Dispute resolution

- Dispute resolution
  - Triggered by a relevant and reasoned objection that is rejected by the lead supervisory authority; or
  - With conflicting views on which of the supervisory authorities is competent for the main establishment; or
  - If a certain decision that should have been submitted is not submitted.

- Decision within 4 weeks with 2/3 majority vote

- **Decision is binding and subject to appeal (by the CJEU and national courts)**