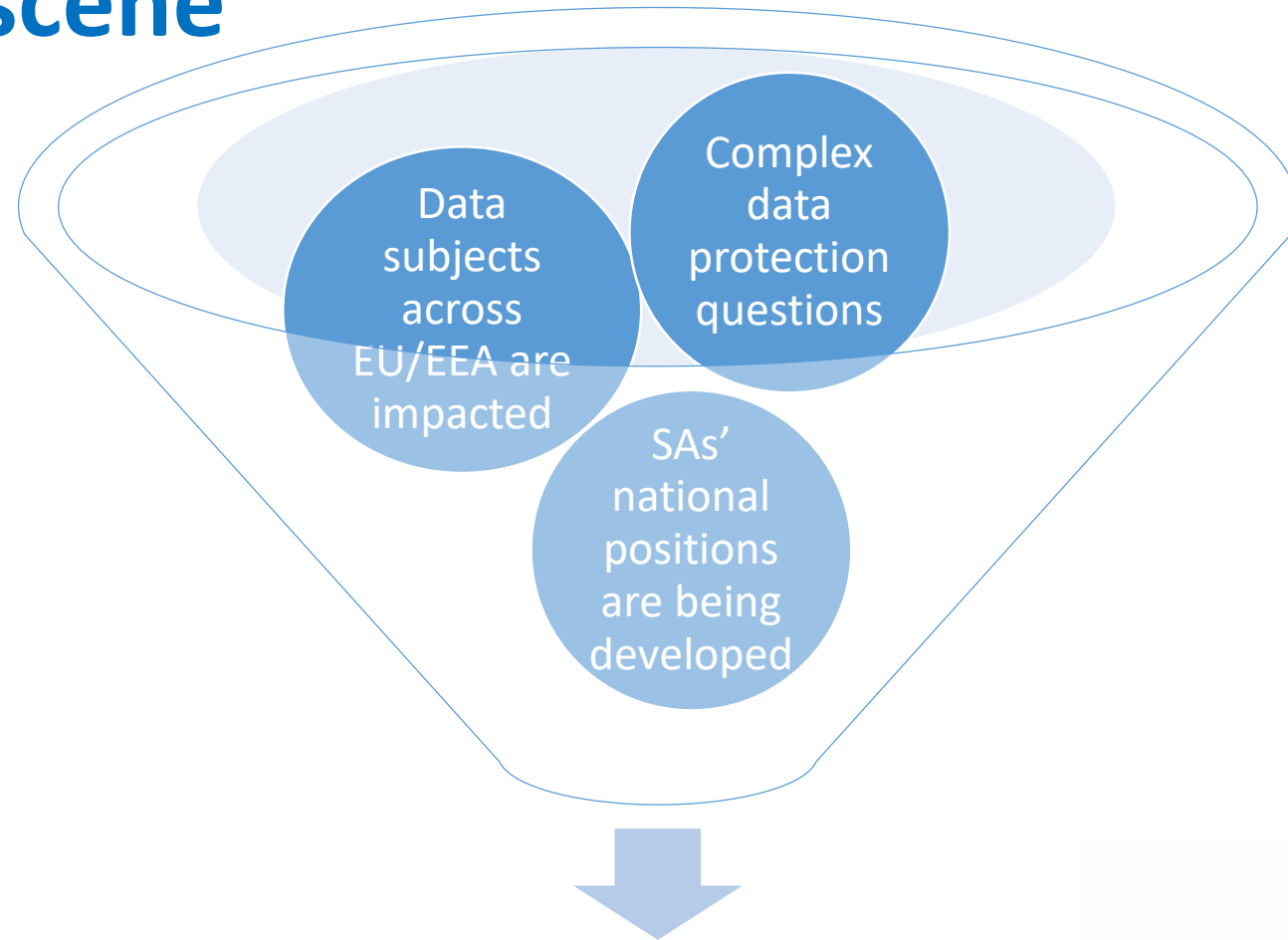


The EDPB Consistency Opinion 28/2024 on AI models

Amandine Jambert & Diletta De Cicco
European Data Protection Board (EDPB) Secretariat

10 April 2025

Setting the scene



IE DPA's request made:

Need to develop a common EU approach

Art.64(2) Opinion : advantages and limits

Scope depends on the request (vs. GL own initiative)

Need for SAs to take utmost account of it when dealing with specific cases > possible Art.65 binding decision

Tight deadlines: 8 weeks (possibility to add 6 weeks if complex)

Complex to consult the public during and not possible after as final

Key issues addressed



1. When and how an AI model can be considered as ‘anonymous’

2. How controllers can demonstrate the appropriateness of legitimate interest as a legal basis in the development and deployment phases

3. What are the consequences of the unlawful processing in the development phase on the subsequent processing or operation of the AI model.

1. AI models as “anonymous”

Why this question in a 64.2?

GDPR applies only to personal data



WP29 Opinion on Anonymization techniques

Full identification risk analysis

or 3 criteria (single out, linking and **inference**)

Elements to help DPAs decide

AI models can be anonymous if it is very unlikely to

1. extract directly personal data used to create the model

2. obtain such personal data from the model through queries.

Elements to assess a claim of anonymity

AI model design

- Measures taken during the design to achieve anonymity:
 - Selection of sources
 - Data preparation and minimisation
 - Methodological choices for training
 - Measures regarding model outputs

AI model analysis

- Internal or external audits

Testing and attack resistance against

- Attribute and membership inference
- Exfiltration
- Regurgitation
- Model inversion
- Reconstruction

Documentation

- DPIAs
- DPO's advice
- Technical and organizational measures
- On theoretical resistance to re-identification and controls

2. Legitimate Interest in the development and deployment phase

General Observations

No hierarchy

between the legal bases
provided by the GDPR

Accountability

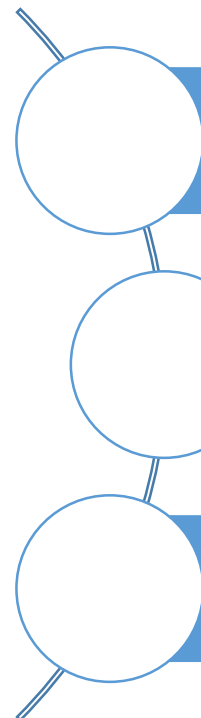
Controllers need to
identify the appropriate
legal basis for their
processing activities

**Compliance with the
general principles
of the GDPR**

**Compliance with data
subjects' rights**

Methodology

3 Steps Test

- 
- The diagram illustrates the '3 Steps Test' methodology. It consists of three white circles arranged vertically, connected by a thin line. Each circle is positioned to the left of a blue rectangular box containing a step number and description. The circles have a small line extending from the top-left and bottom-left, giving them a 3D or pin-like appearance.
1. **Pursuit of a legitimate interest** - Identifying the legitimate interest pursued by the controller or a third party.
 2. **Necessity test** - Analysing the necessity of the processing for the purposes of the legitimate interest(s) pursued.
 3. **Balancing Test** - Assessing that the legitimate interest(s) is (are) not overridden by the interests or fundamental rights and freedoms of the data subjects.

Step 1 – Pursuit of a “legitimate” interest

Legitimate

- Lawful Interest
- Clearly and precisely articulated
- Real and present

Examples:

- Developing a conversational agent
- Detecting fraudulent content or behaviour
- Threat detection in an information system

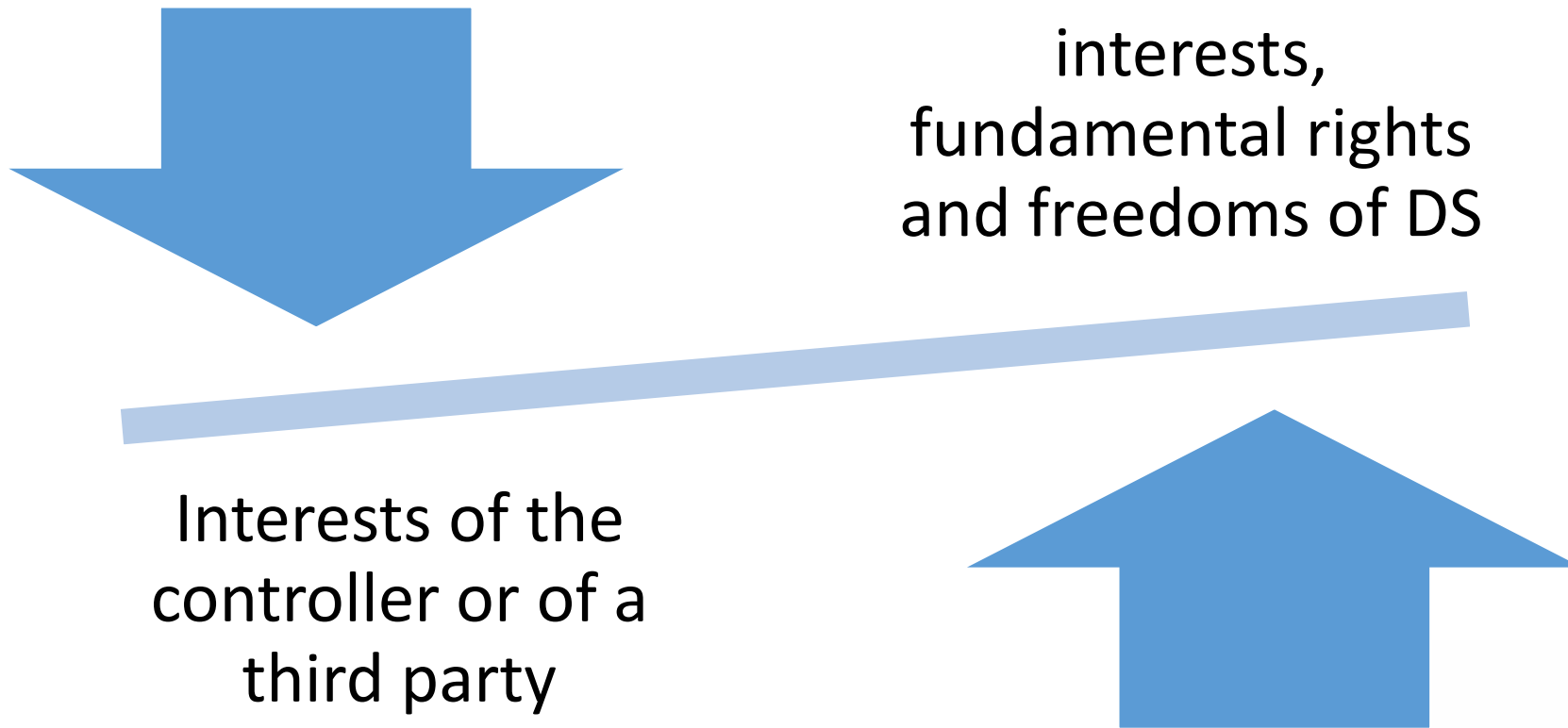
Step 2 - Necessity of Processing

Analyse:

1. if the processing adequate to achieve the purpose pursued; and
2. if there is no less intrusive way of pursuing this purpose.

Implementing technical safeguards may contribute to meet the necessity test.

Step 3 - Balancing test



Step 3 - Elements of the test

1. Data subjects' interests, fundamental rights and freedoms	Taking into account those that can be positively or negatively affected by the processing
2. Impact on data subjects	Taking into account the nature of the data, the context, the further consequences of the processing
3. Reasonable expectations	Important element: info provided, context of processing (data publicly available, nature relation between DS and C, context of collection, service...)
4. Mitigating measures	Technical, facilitating exercise of rights, transparency

3. Impact of unlawful development on subsequent operation of the model

General Observations

Scope

- Non-compliance with the principle of lawfulness (Article 5(1)(a) and Article 6 GDPR).

Accountability

- Controllers must demonstrate compliance with GDPR principles.

SAs' Powers

- SAs have discretionary powers to assess infringements and choose appropriate measures.

3 Scenarios

Unlawful
development
of the model.
Then:

1. personal data is retained in the model
and is subsequently processed by the same controller
at deployment

2. personal data is retained in the model
and is processed by another controller at deployment

3. the model is anonymised,
before the same or another controller initiates another
processing of personal data at deployment

Key Takeaways

- When an AI model was developed with **unlawfully processed personal data**, this could have an impact on the lawfulness of its deployment (subsequent processing), **unless the model has been duly anonymised**.
- **SAs always have the power to intervene with regard to the data processing conducted during the development phase.**

Scenario 1

- Same controller + personal data is retained in the model

There may be an impact on lawfulness of the subsequent processing > Case-by-case assessment needed

For instance: If the subsequent processing is based on legitimate interest, need to consider the initial unlawfulness in the legitimate interest assessment

SAs can impose corrective measures on the initial processing

Scenario 2

- Separate controller – personal data is retained

There may be an impact on lawfulness of the subsequent processing > Case-by-case assessment needed

Each controller should ensure the lawfulness of the processing it conducts

The controller deploying the model should conduct an appropriate assessment to ascertain that the model was not developed unlawfully

Scenario 3

- Anonymisation before deployment

If the model has been anonymised, GDPR does not apply to the anonymised model (but the bar is high).

Hence, unlawfulness of the initial processing should not impact the subsequent operation of the model.

EDPB Work on AI

What are we working on and what's next?

1. Guidelines on the Interplay between the AI Act and the EU data protection legislation
2. Guidelines on web scraping
3. Task force to Generative AI Enforcement
5. International cooperation, e.g. G7 Roundtable of DPAs
6. Support Pool of Experts projects

Thank you !

For further information:

- The EDPB website: <https://edpb.europa.eu/>
- Follow us on social media:



<https://www.linkedin.com/company/eu-edpb/>



@eu_edpb

