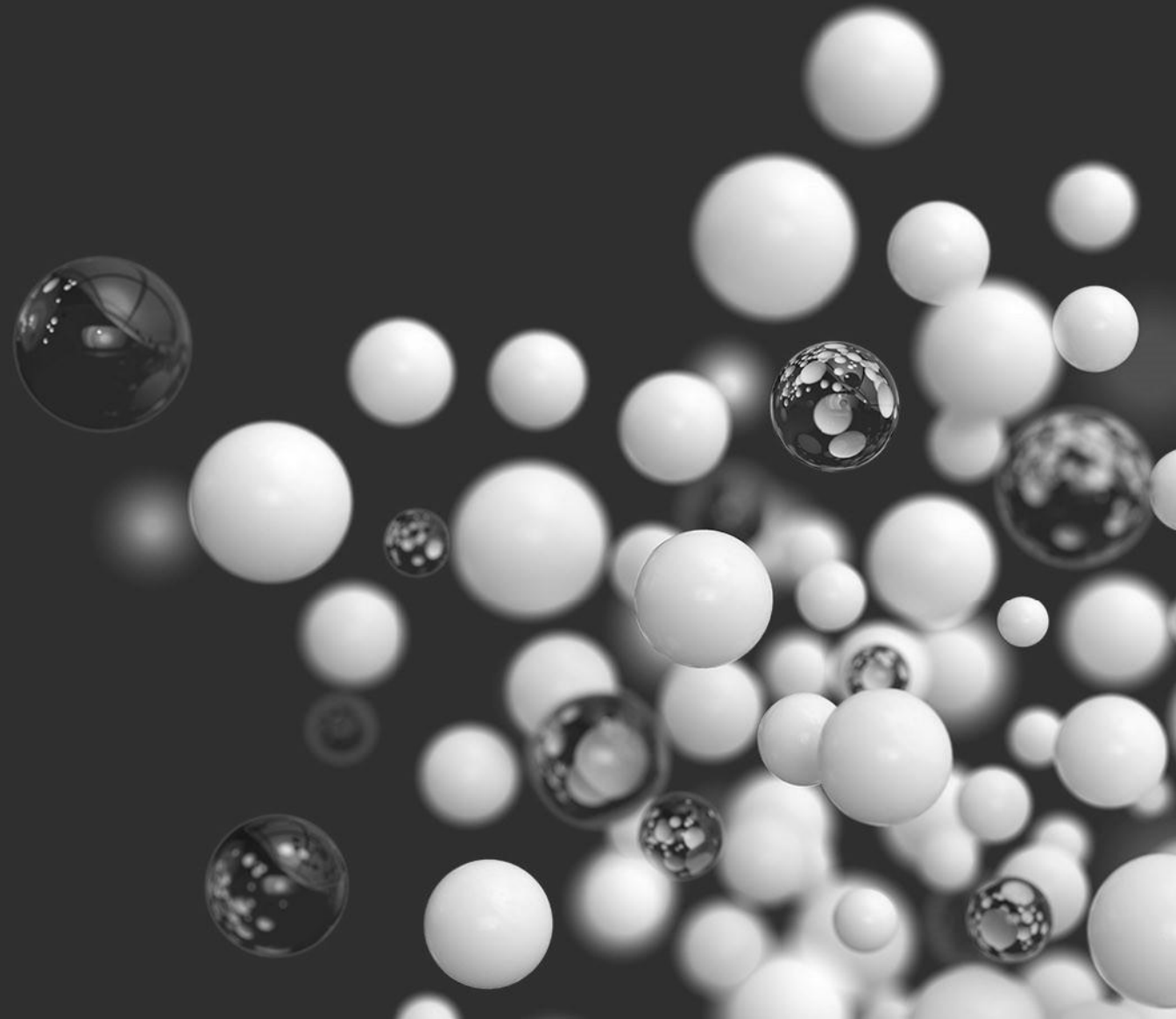
Data Privacy Landscape in the EU

Speakers
Alejandro Guerrero
Minesh Tanna
Sarah Bailey
Jérémie Doornaert

25 October 2023



Overview

Agenda

Alejandro Guerrero
Partner
Brussels,Belgium

Minesh Tanna
Partner
Global AI Lead
London,UK

Sarah Bailey
Partner
Paris, France

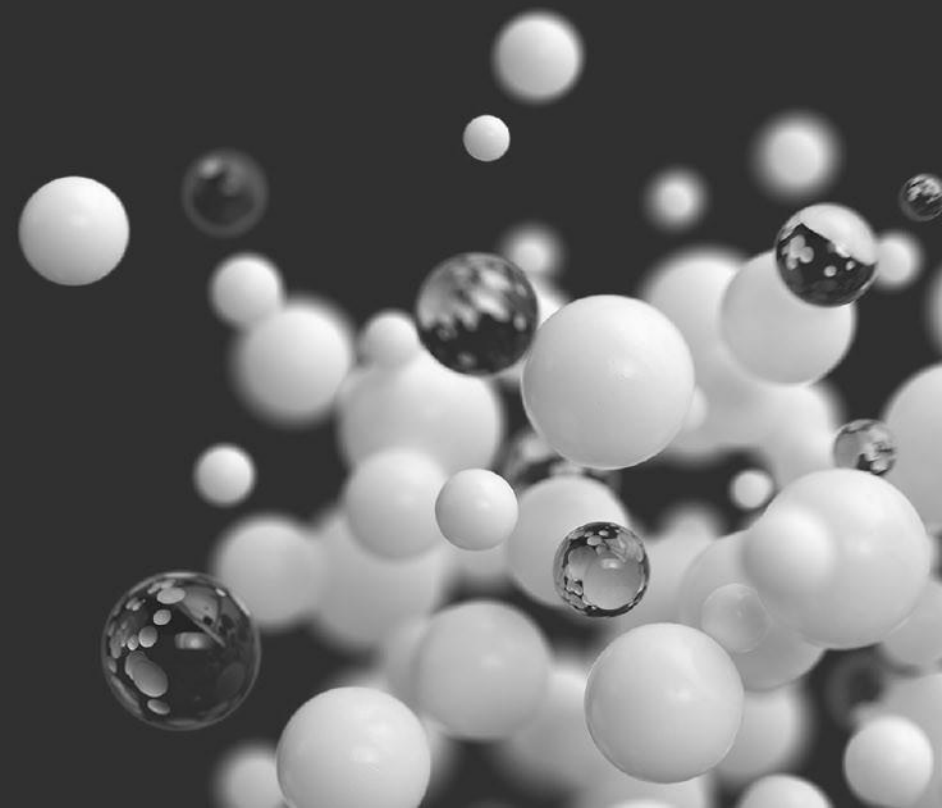
Jérémie Doornaert
Managing associate
Brussels,Belgium

1 Introduction

2 GDPR and AI Act

3 GDPR and DSA

Introduction



Regulating Tech Beyond Privacy

§

- Over 10 years since the EC proposed the GDPR Bill, in 2012, and 5 years since it became applicable, the GDPR has fundamentally changed the way in which companies process personal data

- The GDPR also kicked off a period of intense legislative activity to further regulate data and technology:

Cybersecurity and Data-Related Legislation

E-Privacy Regulation (Proposal)

Regulation on Free Flow of Non-Personal Data

Cybersecurity Act and NIS 2 Directive

European Governance Act

European Data Act (Proposal)

Other General Behavioural Legislation with Data Aspects

AI Act (Proposal)

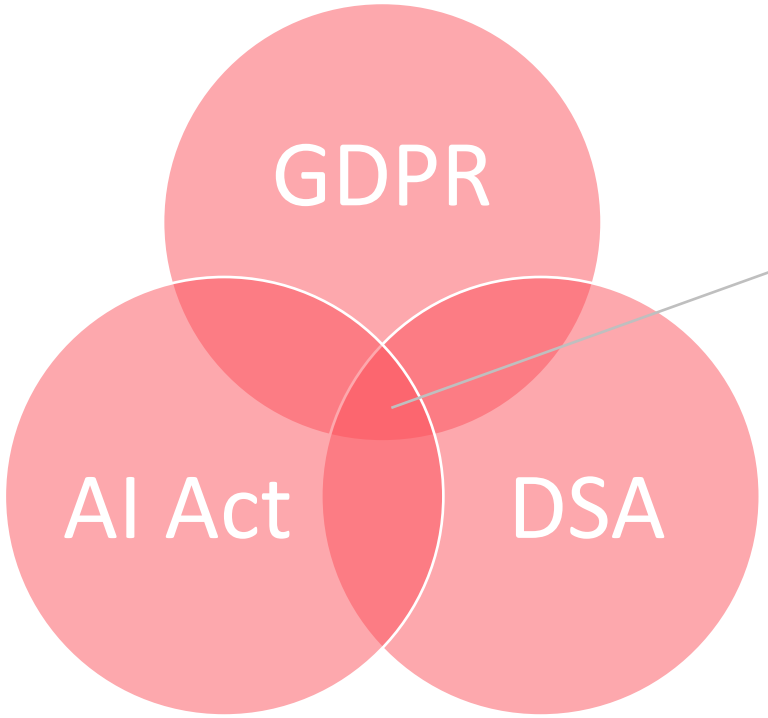
Digital Services Act (DSA)

Specific Behavioural Legislation with Data and Economic Aspects

Digital Markets Act (DMA)

The GDPR's Interplay with the AI Act and DSA

- The GDPR affects and is impacted by other EU legislation, in particular, the AI Act and the DSA
- This overlap raises questions about parallel substantive application, governance and enforcement



Substantive application, eg:

- Identification of illegal content
- Dark patterns
- Online advertising

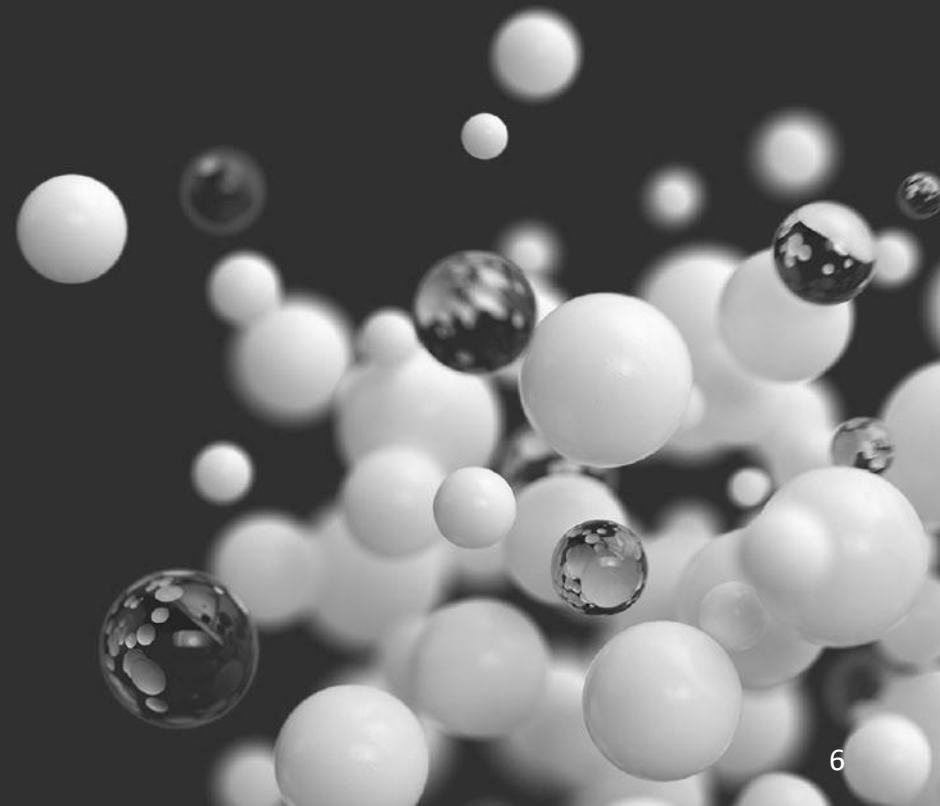
Governance, eg:

- Polices on DPIAs, Risk Assessments, AI Conformity Assessments
- Compliance functions and officers

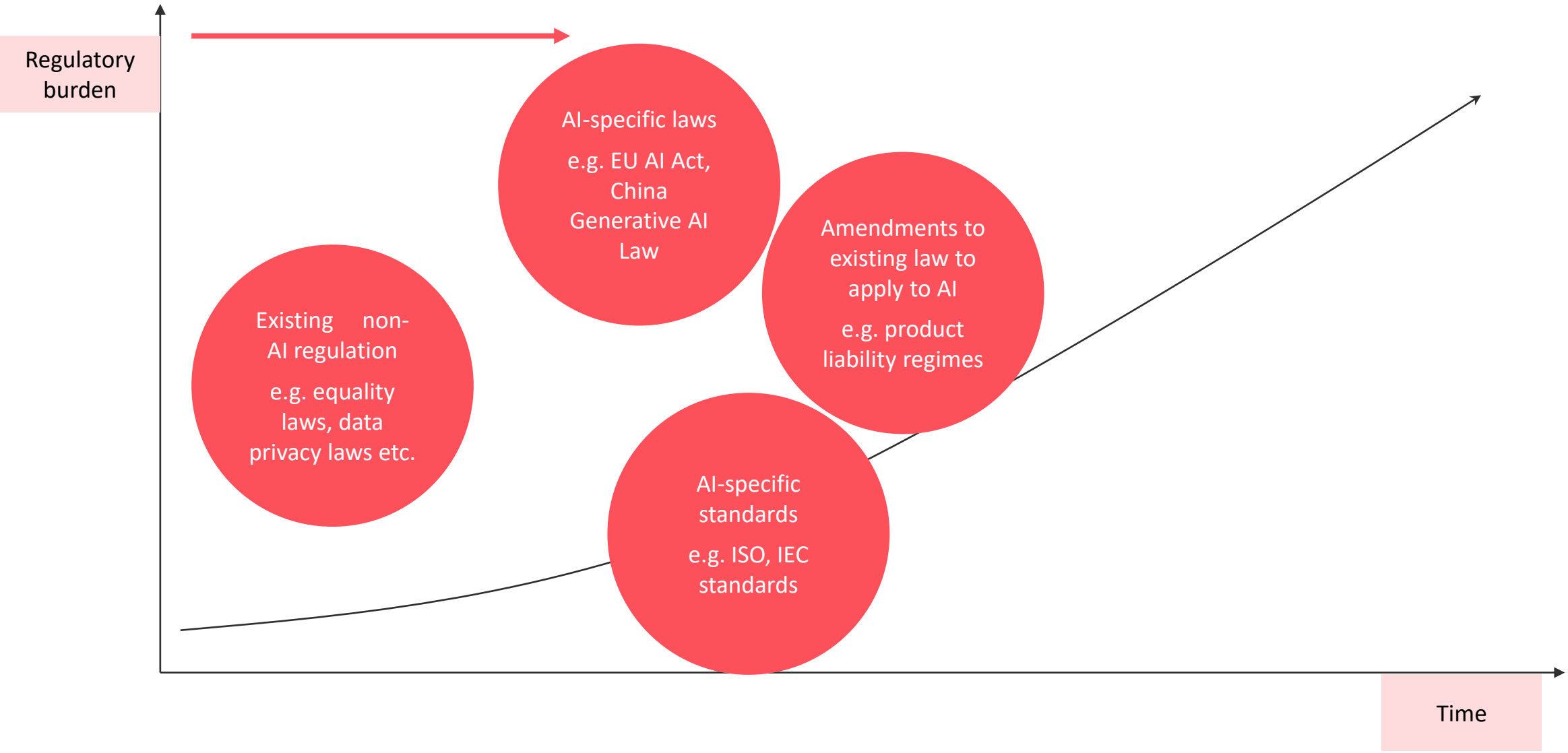
Enforcement:

- SAs, DSCs and AI NSAs.

GDPR and AI Act



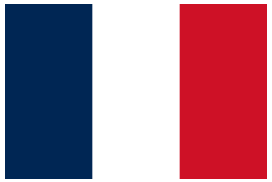
Direction of AI Regulation: Sources / Type



Regulatory / legal action: examples

Class action against Stable Diffusion and Midjourney

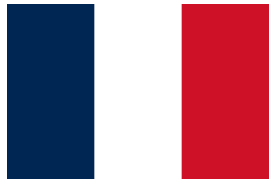
Class actions against Open AI



French DPA fines Clearview AI

Class action by Getty Images against Stable Diffusion

Class action against Google

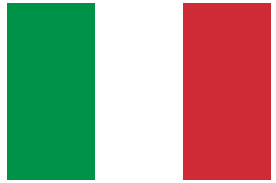


Complaints filed about ChatGPT to French DPA

FTC investigating ChatGPT

Office of Privacy Commissioner investigating ChatGPT

Spanish DPA probing ChatGPT



ChatGPT investigated by Italian DPA

Defamation lawsuit regarding Chat GPT

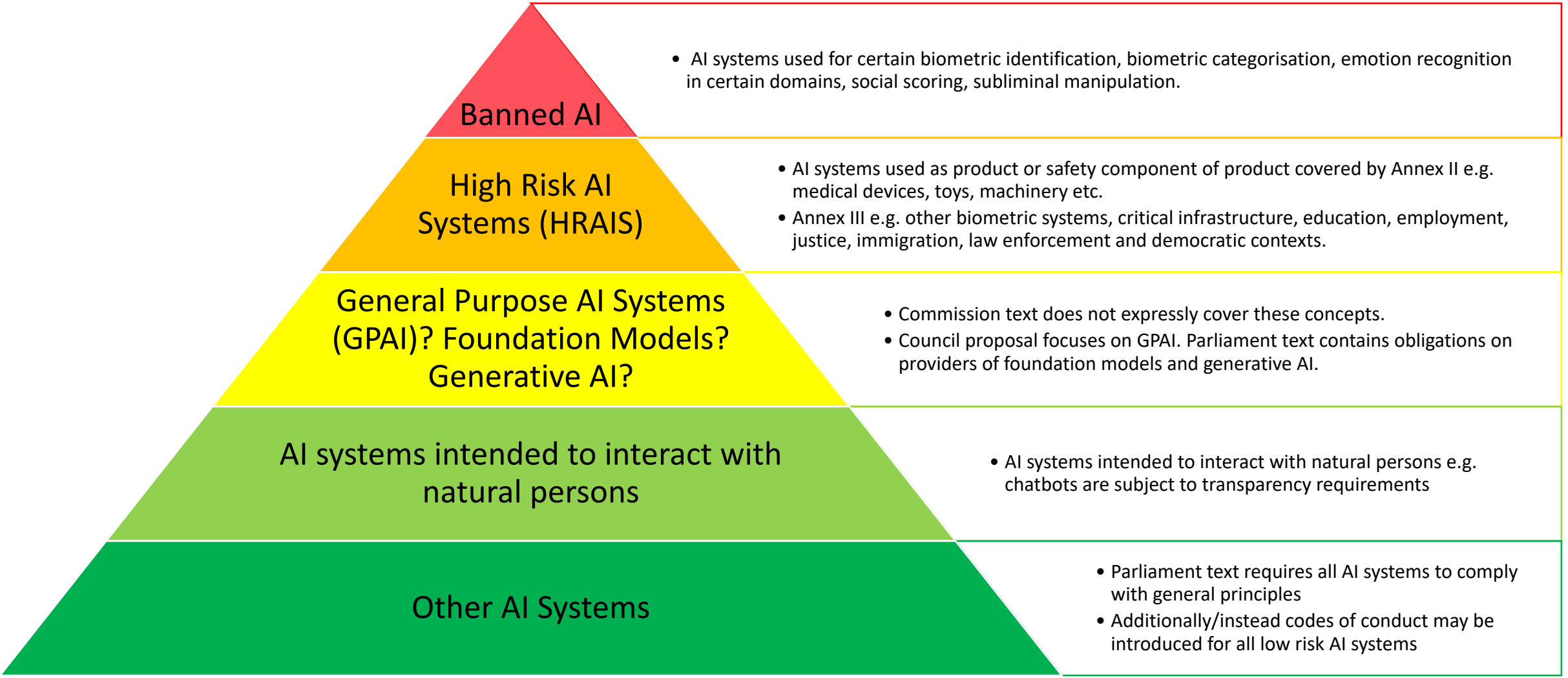
German DPA looking at ChatGPT

Japan privacy watchdog warns OpenAI

EU AI Act: Key Points

- Binding regulation, following EU's 'New Legislative Framework' for product safety, comprising harmonised requirements, certification, market monitoring rules and enforcement through EU and Member State bodies
- Horizontal application, with risk-based approach
- Substantive and procedural obligations
- Regulatory burden higher on providers / developers than on users / deployers
- Extra-territorial
- EU enforcement network with high fines for non-compliance
- Final text expected end-2023, with 2-year implementation period thereafter

EU AI Act: Structure



Overlap between the GDPR and EU AI Act

- Both about protecting individuals' rights
- AI systems which process personal data during training or deployment
- Fairness, transparency, accuracy and accountability principles under GDPR are also core part of EU AI Act
- AI systems undertaking solely automated decision-making
- Biometric systems are high-risk under EU AI Act and use special category data under GDPR

BUT, there are fundamental differences:

- Types of harm that each seeks to protect varies (e.g. privacy v fundamental rights)
- Focus on use of personal data v development / use of tech

Consider the relationship between a law which governs the use of fuel and a law which governs the development / use of motor vehicles

Relevance of GDPR for AI systems

§

GDPR is technology neutral. It applies to any "processing of personal data".

"Processing" has a very broad definition under the GDPR:

> *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"*

AIs need data sets to be calibrated, to learn and be developed and to create output

- Those activities are each a processing

Data sets are key for AI development and use. Data sets may include "personal data".

"Personal data" has a very broad definition under the GDPR:

> *"means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"*

- Coded or pseudonymised personal data are within scope of the above definition
- Only anonymized data are excluded

Interplay between draft AI Act and GDPR

- GDPR and AI Act are both grounded on article 16 TFEU which mandates the EU to lay down the rules relating to the protection of individuals with regard to the processing of personal data.

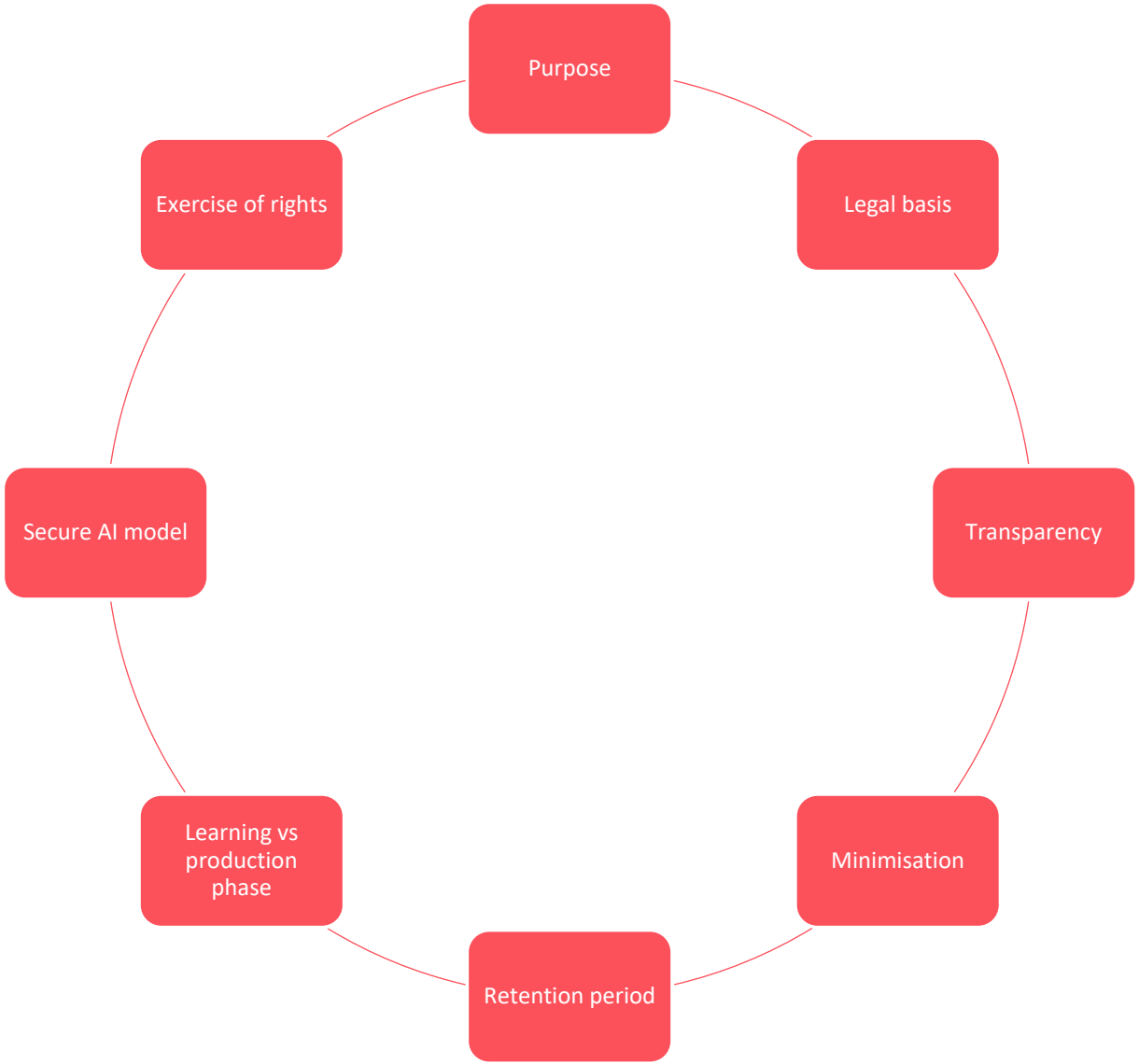
- The draft AI Act "*is without prejudice and complements the GDPR" (*AI Act's Explanatory Memorandum).

  - AI Act's rules will complement the protections afforded to data subjects under the GDPR

  - GDPR applies to development of AI systems using personal data for their design, developments and implementation

  - GDPR applies to processing of personal data impacting an individual (e.g. solely automated decision-making)

Key obligations of GDPR for AI systems



Any lessons from GDPR compliance for AI Act compliance?

§

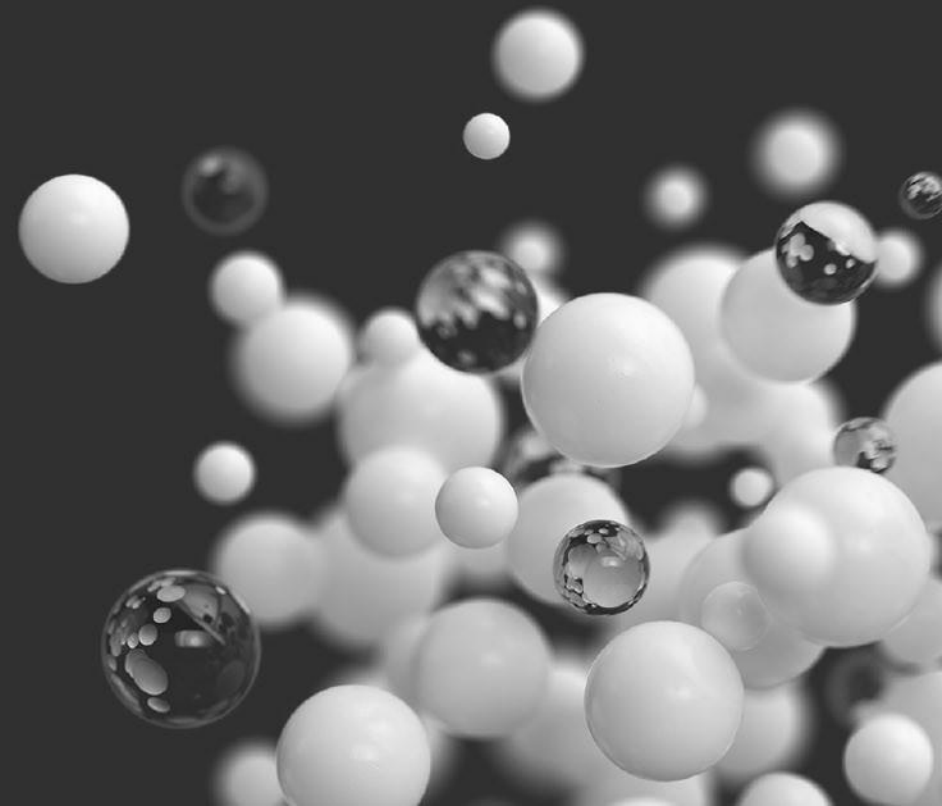
- **Extra-territorial** scope and **EU-based representative**
- Controllers and processors must implement **data privacy by design and by default** taking the challenges of AI into account and applying the 7 principles of GDPR throughout the process
- GDPR and AI Act are pieces of legislation that require **planning**, **transparency** towards persons, **risk assessments** and **documentation**
- Building on an existing **GDPR compliance framework, policies and processes** for managing personal data can provide a foundation for responsible data use and increase cost efficiency when working towards compliance with the AI Act, e.g.:
  - Systematic data mapping
  - Integrated incident and notification management policies (Article 33 GDPR / Article 62 draft AI Act)
  - Information notices (transparency) (Articles 13 & 14 GDPR / Article 11,13 & 14 draft AI Act)
  - DPIA and legitimate interest assessment

Any obligations under AI Act allowing to increase GDPR compliance?

Users may use the information obtained from providers under Article 13 AI Act and the High-Risk AI Systems' (HRAIS') technical documentation to

- comply with their duty to carry out a **DPIA**
- ensure broader alignment with the GDPR and its **transparency requirements**
- provide notice to data subjects about **profiling and automated decision-making**
- complete their **records** of AI-powered **data processing activities** under Article 30 GDPR

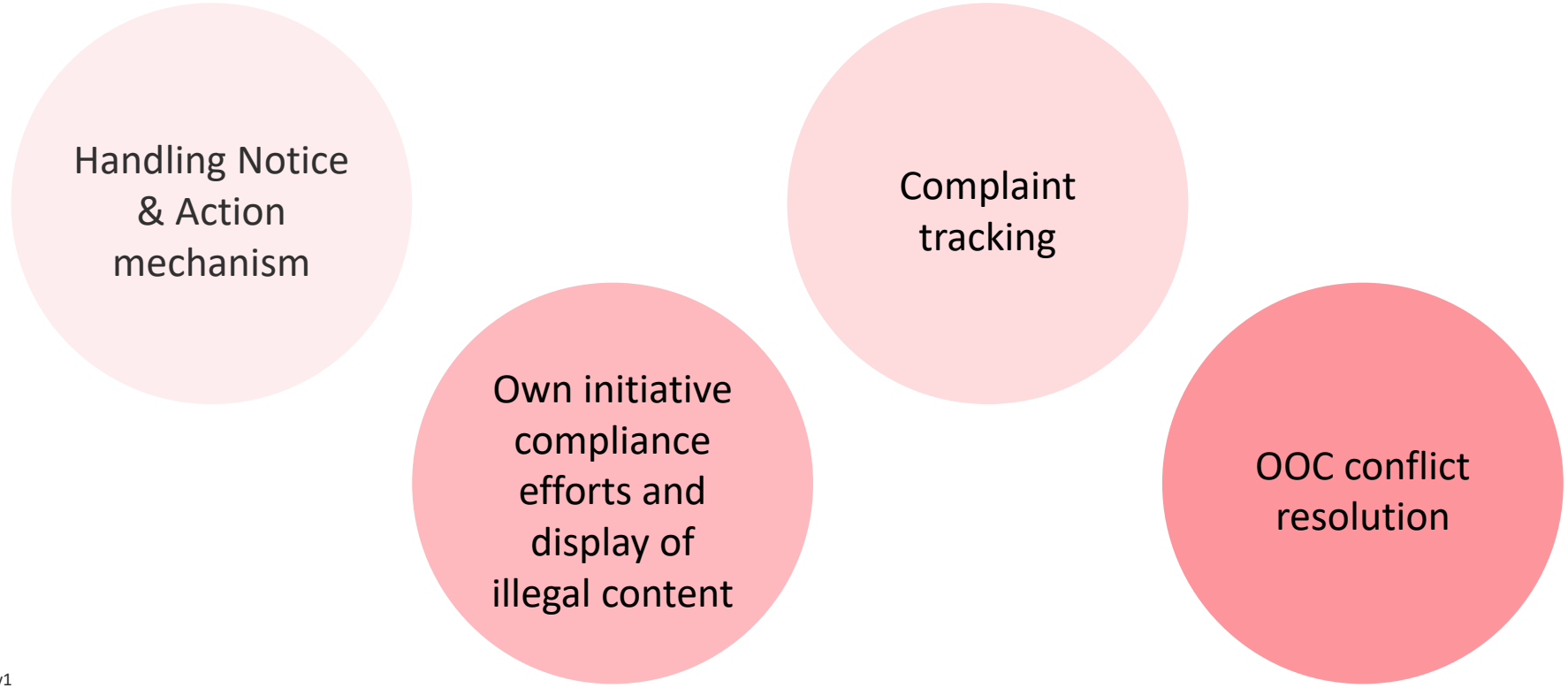
GDPR and DSA



New Data Processing Activities under the DSA

§

- The DSA creates new obligations for hosting service providers, online intermediaries and VLOPs/VLOSEs that require processing of personal data
- GDPR obligations apply to personal data processing operations derived from these DSA provisions



Personal Data Processing & DSA Compliance: Detecting Illegal Content

1. **Own initiative investigations and implement measures to avoid illegal content**

- Article 7 allows companies to put in place measures to detect illegal content – these processes might lead to the processing of personal data
- Certain EU rules aim at exempting/covering some efforts against certain types of illegal content (e.g., child sexual abuse material, see CSAM Prevention Regulation proposal)

- Sophisticated personal data processes can assist companies to eliminate illegal content:
  - Asset-based data processing – such as metadata of content, AI analysis of content (which entails AI improvement by processing other related data)
  - Server-based data processing – data on number, frequency, and patterns of visits to certain websites, that may reflect a participation in hosting illegal content
  - Client-based data processing – data on users and their devices, showing certain browsing behaviour, patterns or connections with others that may raise suspicions

- Deploying any of these measures would require a careful GDPR-compliance assessment, including reviewing the legal basis, transparency obligations, and performance of DPIAs

Personal Data Processing & DSA Compliance:

Dark Patterns

2) Prohibition of dark patterns

- Article 25 prohibits online platforms to design, organize or operate interfaces with dark patterns

- Data protection questions raised:
  - Interface design and display options might be based on an analysis of user data – companies must ensure users are informed of the possible use of their data for product improvement or similar acceptable purposes

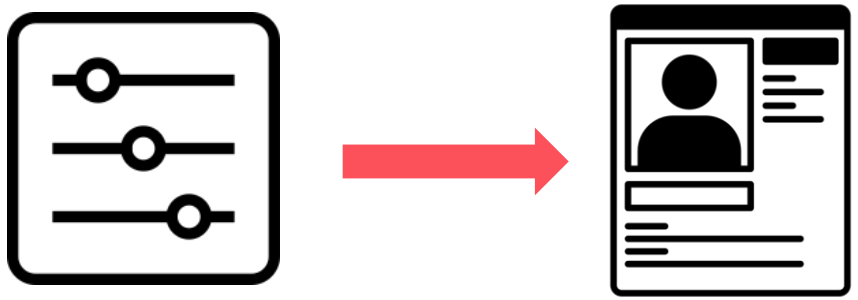
  - (Dark) patterns may rely on data processed from users, e.g., based on browsing behaviours, interests, etc. needing to ensure:
    1. GDPR compliance: personal data is processed lawfully
    2. AI Act compliance: the pattern is not prohibited nor high risk
    3. DSA compliance: the pattern is not dark/prejudicial for consumers

Personal Data Processing & DSA Compliance: Online Advertising and Recommender Systems

§

3) Regulation of online advertising and recommender systems

- Articles 26 and 27 impose obligations on recommender systems and online advertising. In this regard:
  - Information/explainability requirement that may overlap with transparency obligations of the GDPR
  - The ability of users to modify parameters may also influence a company's' ability and purpose of processing data for online advertising/recommender systems – any modification of these parameters may have an impact on what user data can be processed legitimately.



simmons+simmons

Thank you!