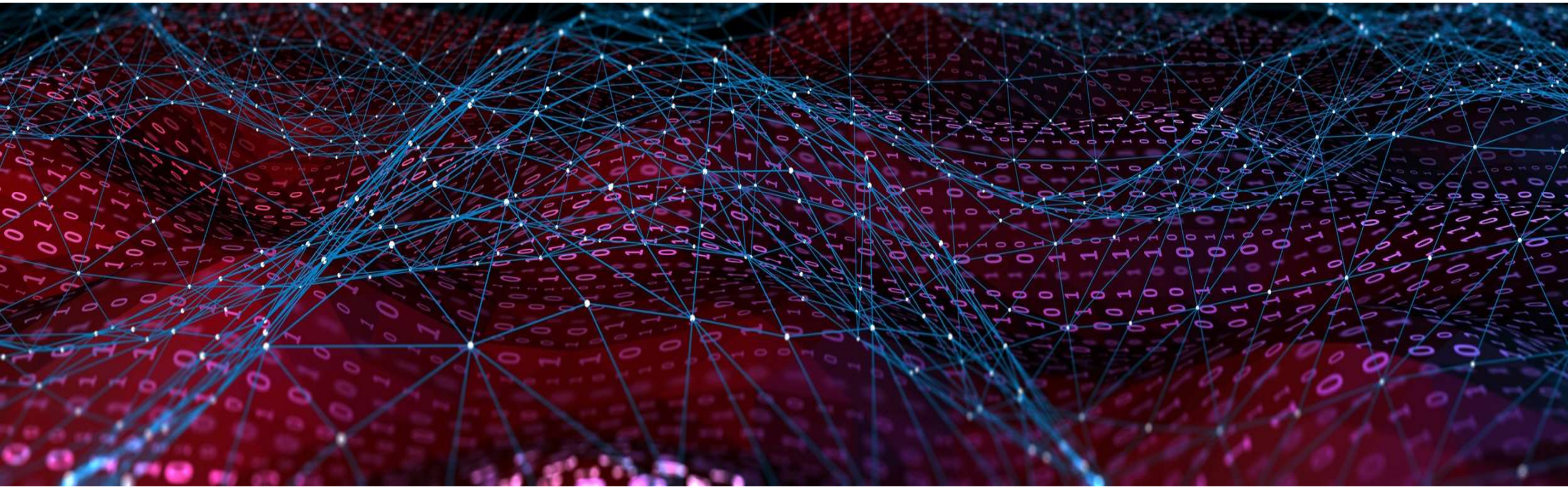
ACC Deal or No Deal
EU AI Act

Simmons & Simmons

Introduction



Speakers and Agenda

Emily Jones
Partner – Head of US Office
T +1650 436 9350
E Emily.Jones@simmons-simmons.com

Christopher Goetz
Partner – Digital Business (Germany)
T +49 8920877 63 32
E Christopher.Goetz@simmons-simmons.com

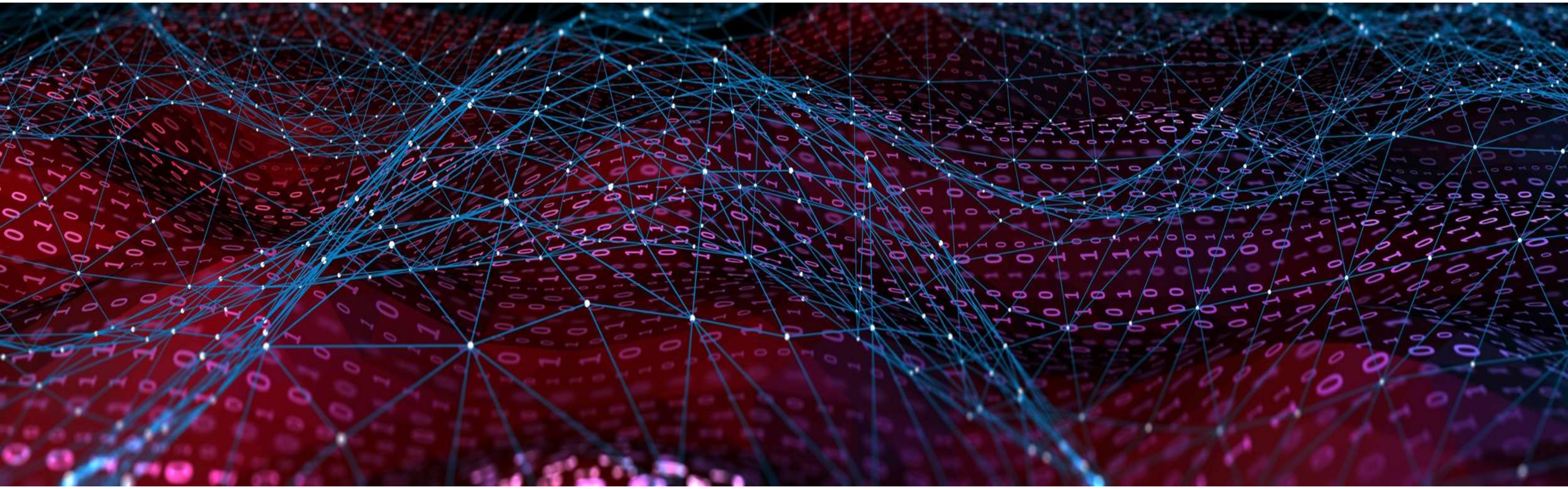
Minesh Tanna
Partner – Disputes and Investigations (UK)
T +44 20 7825 4259
E Minesh.Tanna@simmons-simmons.com

Drew Winlaw
Partner – Solutions (UK)
T + 44 20 7825 5823
E Drew.Winlaw@simmons-simmons.com

Agenda

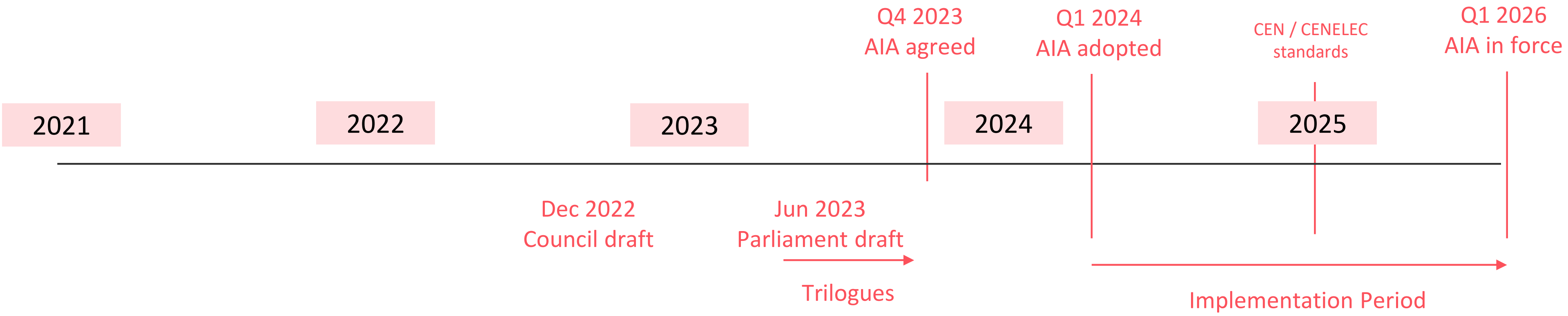
- Introduction to the EU AI Act
- Case studies: application to US companies
- AI implementation challenges
- Interaction with GDPR
- Q&A

Introduction to the EU AI Act



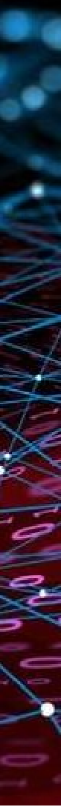
Origins and latest status

- In 2019, President von der Leyen promised EU regulation on AI. European Commission published draft AIA in Apr 2021, following white paper.
- European Parliament adopted amendments to draft AIA on 14 Jun 2023, following European Council's proposed amendments in Dec 2022
- Final AIA text now being negotiated (so-called 'trilogues')
- Timeline, with anticipated future steps:



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
- Focus on risky uses, but also now on risky forms of AI technologies
- 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



Definition of "AI system"

Commission Draft

AI system means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.

…

(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

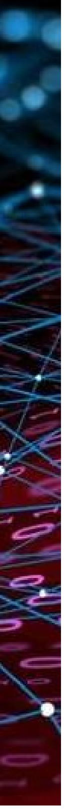
(c) Statistical approaches, Bayesian estimation, search and optimization methods.

Council Proposal

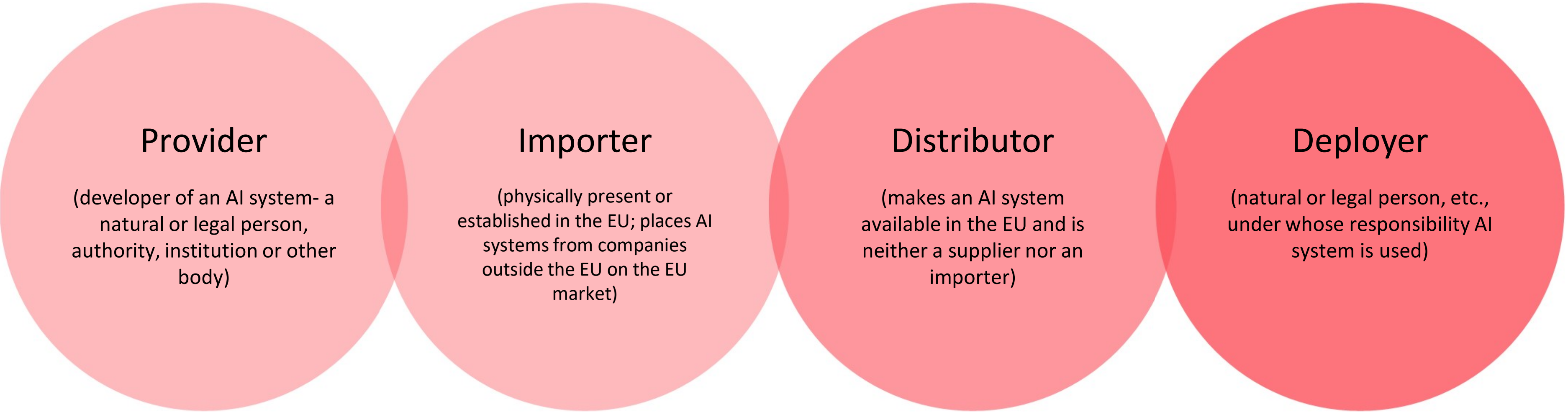
AI system means a system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts.

Parliament Text

AI system means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments.



Stakeholders



Provider

(developer of an AI system- a natural or legal person, authority, institution or other body)

Importer

(physically present or established in the EU; places AI systems from companies outside the EU on the EU market)

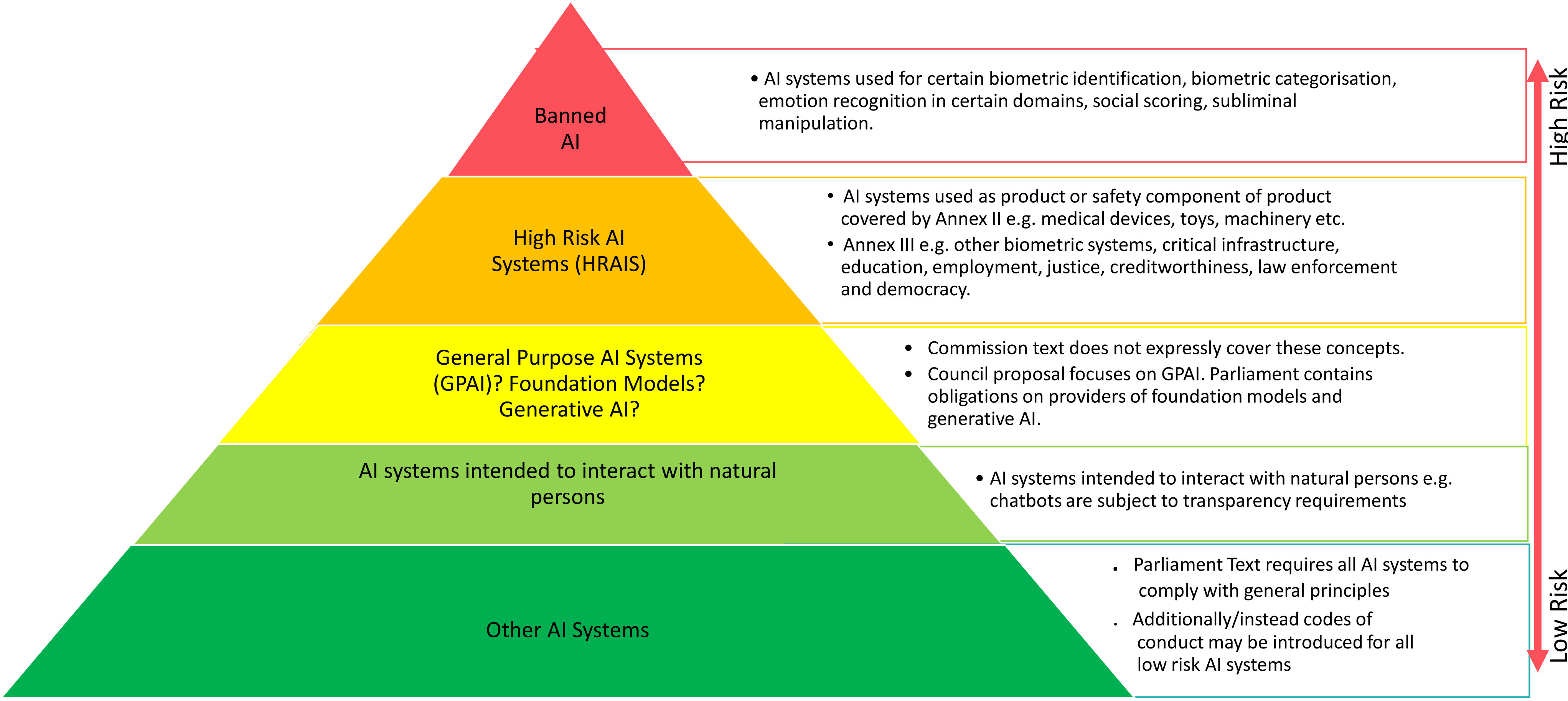
Distributor

(makes an AI system available in the EU and is neither a supplier nor an importer)

Deployer

(natural or legal person, etc., under whose responsibility AI system is used)

Risk-based approach



Banned AI

- AI systems used for certain biometric identification, biometric categorisation, emotion recognition in certain domains, social scoring, subliminal manipulation.

High Risk AI Systems (HRAIS)

- AI systems used as product or safety component of product covered by Annex II e.g. medical devices, toys, machinery etc.
- Annex III e.g. other biometric systems, critical infrastructure, education, employment, justice, creditworthiness, law enforcement and democracy.

General Purpose AI Systems (GPAI)? Foundation Models? Generative AI?

- Commission text does not expressly cover these concepts.
- Council proposal focuses on GPAI. Parliament contains obligations on providers of foundation models and generative AI.

AI systems intended to interact with natural persons

- AI systems intended to interact with natural persons e.g. chatbots are subject to transparency requirements

Other AI Systems

- Parliament Text requires all AI systems to comply with general principles
- Additionally/instead codes of conduct may be introduced for all low risk AI systems

Extra-territoriality

- Act will apply to
  - users of AI systems located within the EU
  - providers placing on the market or putting into service AI systems in the EU, even where they are established outside of the EU
  - providers and deployers of AI systems that are located outside of the EU, where the "output produced by the system is used in the [EU]"

Stakeholders – Obligations

Provider

(developer of an AI system- a natural or legal person, authority, institution or other body)

Deployer

(natural or legal person, etc., under whose responsibility AI system is used)

Provider obligations re high-risk AI systems (Art. 16)

Risk management

Implementing process for entire lifecycle of HRAIS to identify, analyse and mitigate risks

Article 9

Data quality / Data Governance

Training and testing of HRAIS using data shall be undertaken in accordance with

Article 10

Technical Documentation

Drafting comprehensive "manual" for HRAIS which contains, at a minimum the Annex IV informatio

Article 11

"Record-keeping"

HRAIS must be designed to ensure automatic logging of events eg period of use and input data reviewed (Article 12) and providers must keep these logs

Article 20

Transparency / Explainability

HRAIS must be accompanied by instructions for use which include detailed information including their characteristics, capabilities and limitations, *Article 13*

"Human oversight"

HRAIS must be designed so they can be overseen by humans, who should meet various requirements eg being able to understand the HRAIS and to stop its use

Article 14

Accuracy, resilience and cyber security

HEAIS must be accurate (with accurac metrics included in instructions for use), resilient to errors or inconsistencies (eg through fail-safe plans) and resilient to cyber-attacks

Article 15

Quality - Management Systems

HRAIS providers must put in place a comprehensive quality management system which includes at least the extensive information requirements

Article 17

Conformity assessment

HRAIS provider shall follow conformity assessment procedure

Article 43

"Post-marketing monitoring"

HRAIS providers must document a system to collect and analyse data provided by users on the performance of the HRAIS throughout its lifetime

Article 61

Provider obligations re high-risk AI systems

Data quality / Data Governance

Training and testing of HRAIS using data shall be undertaken in accordance with

Article 10

Key provision!

- ➢ Training data = basis of any AI System
- ➢ Insufficient quality of training data:
  - □ Negative impact on functioning of AI System
  - □ Output may be incorrect
  - □ Bias as a result

Sanctions: Violation of Provider obligations

□ Violation of provider obligations "**Data Quality**" (Art. 10) and "**Transparency**" (Art. 13)

up to

- EUR 20 million or, in the case of a company,
- **4 % of** the annual worldwide turnover of the previous marketing year

□ Violation of **any other provider obligation** (listed in Art. 16):

up to

- EUR 10 million or, in the case of a company,
- **2 % of** the annual worldwide turnover of the previous marketing year

Stakeholders – Obligations

Provider

(developer of an AI system- a natural or legal person, authority, institution or other body)

Deployer

(natural or legal person, etc., under whose responsibility AI system is used)

Obligations for Deployers of high-risk AI systems (Art.29)

□ **"AI Literacy"** (Art. 4b)

- Teaching basic notions & skills about AI systems, risks & benefits to staff
- "Sufficient level of AI literacy" = ability of deployer to ensure compliance with AI Act

□ **Compliance with "General Principles"** (Art 4a)

- e.g. compliance with GDPR / continuous monitoring / event logging

□ **"Fundamental rights impact assessment" prior to putting system into use (Art. 29a)**

- **Intended purpose of use**
- **Categories of natural persons to be likely affected**
- **Reasonable foreseeable adverse impact of use of system**
- **Description of governance system (incl. human oversigh ress)**
- **Detailed plan on risk mitigation**

Jointly with
Art. 35 GDPR
Data Protection
Impact Assessment
(where applicable)

Sanctions: Violation of Deployer obligations

Violation of **any deployer obligation:**

up to

- EUR 10 million or, in the case of a company,
- **2 % of** the annual worldwide turnover of the previous marketing year

Foundation Models (GPT-4 et al)

□ Foundation models:

- **all models**: transparency obligations
- **"very capable" models**: red-teaming through vetted red-testers, risk assessment/mitigation and regular compliance controls through independent auditors.

➢ **"very capable" models**: threshold to be introduced that triggers (rebuttable) assumption that model is "very capable" (e.g. compute power used to train model in FLOPS)

□ Copyright:

Providers must:

- respect rights holders' opt-out right from content to be used for training purposes
- make publicly available sufficient detailed summary re content used for training & policies to manage copyright-related aspects

General Purpose AI (ChatGPT et al)

GPAI systems:

- **all provider of GPAI systems**:
  - explicit statement whether GPAI can be used for high-risk uses.
  - where high-risk is excluded: measures to detect and prevent such use need to be introduced.
  - where high-risk is allowed: GPAI system needs to comply with requirements for high-risk AI systems.
- **GPAI systems used "at scale" in EU**:
  - subject to regular red-teaming through vetted red-testers & risk assessment/mitigation.

- **GPAI system used "at scale“?**
  - impact and reach relevant.
  - relevant threshold proposed: 10,000 registered business users (i.e. developers) or 45 million registered end users.

(Note for comparison: ChatGPT has currently approx. 100+ million end users.)

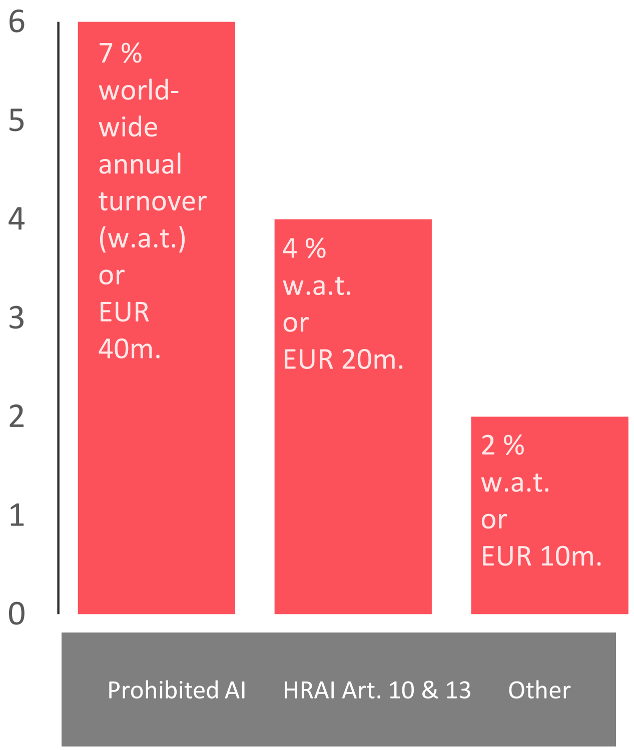
Enforcement of the AI Regulation/Sanctions

- □ **National authorities** **(**to be determined by each EU member state)
- □ New "**AI Office"** (hosted within EU Commission)
  - ➢ EU-wide enforcement of new rules on foundation models & GPAI systems

> ***"Being the first body worldwide with powers to enforce rules on foundation models and GPAI, the AI Office would become an international reference point for AI governance."***

Liability

- Sanctions, Art. 71 AI Act.



→

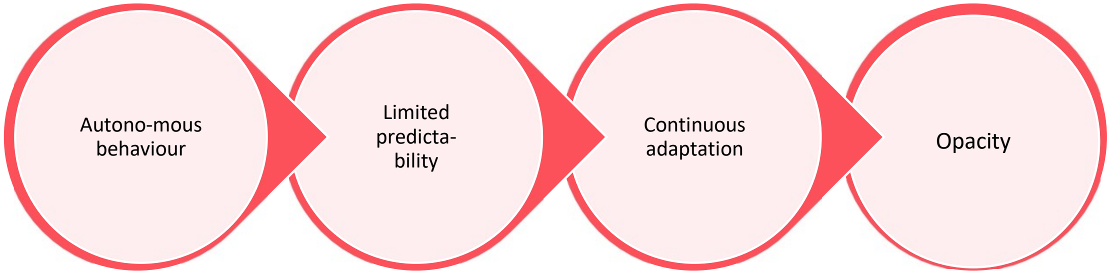
- Civil liability?

✗

But…

Adaption of liability regulations to the digital age

EU Commission: **Characteristics of AI** make it difficult to claim damages



Autono-mous behaviour

Limited predicta-bility

Continuous adaptation

Opacity

Further: "Costly to prove **damage** and **causality** (due to lack of technical expertise)“
(→ burden of proof on side of claimant!)

28 September 2022:

➢EU Commission proposed an EU **Directive** adapting the rules on **civil liability to artificial intelligence** (AI Liability Directive)

AI Liability Directive (draft)

Easier to enforce damage claims in respect of
High-risk AI systems

Broad disclosure obligations **for providers/deployers of AI systems alleged** to have inflicted harm

(reversal of burden of proof!)

if no disclosure:

(rebuttable)

presumption of fault

(rebuttable)

presumption of a causal link

in event of a

<u>fault</u>

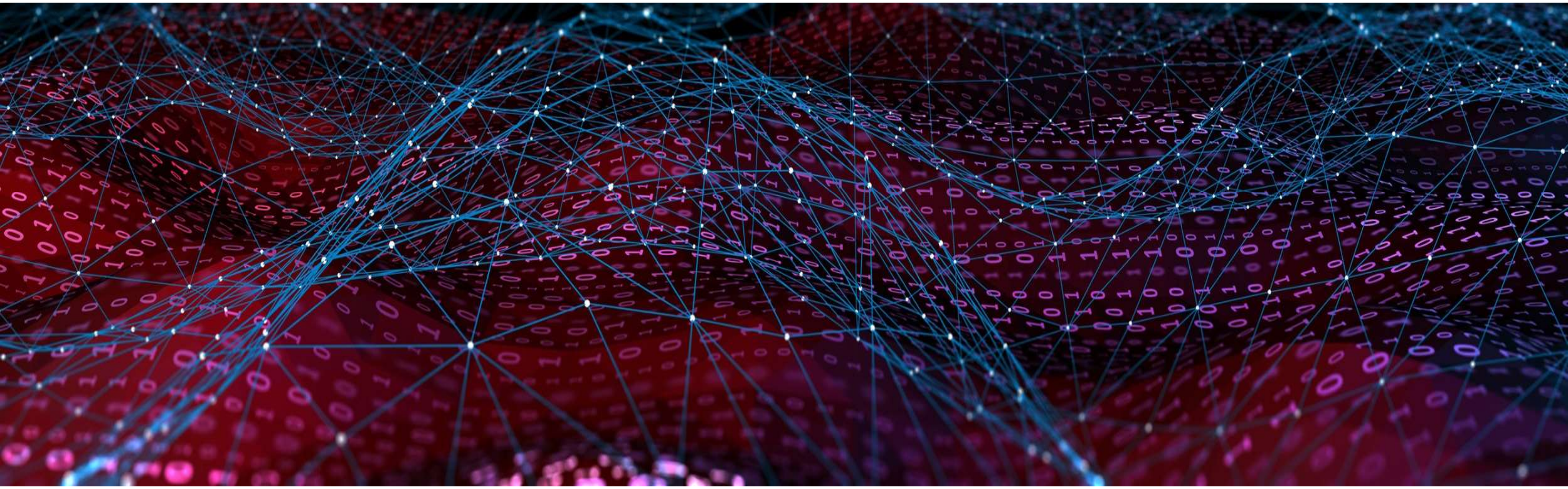
"Fault" on the side of provider if:

- Data quality (-)
- Transparency (-)
- Cybersecurity (-)

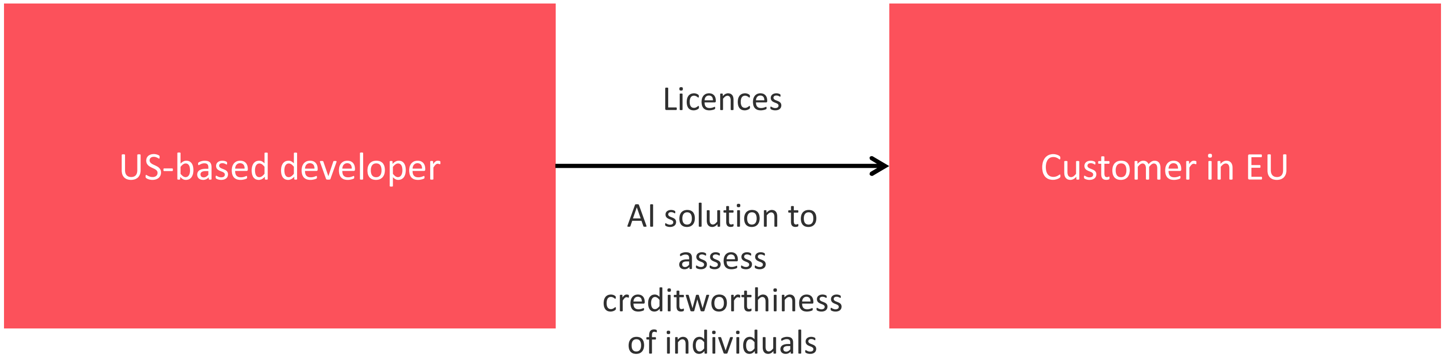
"Fault" on the side of deployer if:

- Used according to instructions for use (-)
- Input data contradict purpose

Case Studies



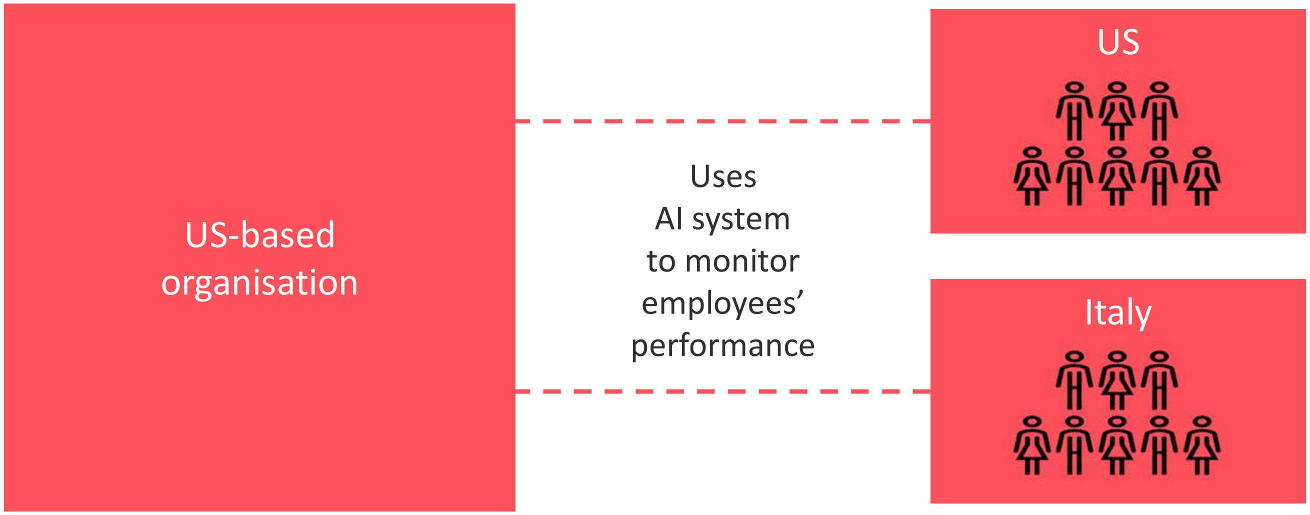
Case study 1: US developer



"placing on the market … AI systems in the EU, even where they are established outside of the EU"

Article 2(i)(a)

Case study 2: US deployer with EU Employees



US-based organisation

Uses AI system to monitor employees' performance

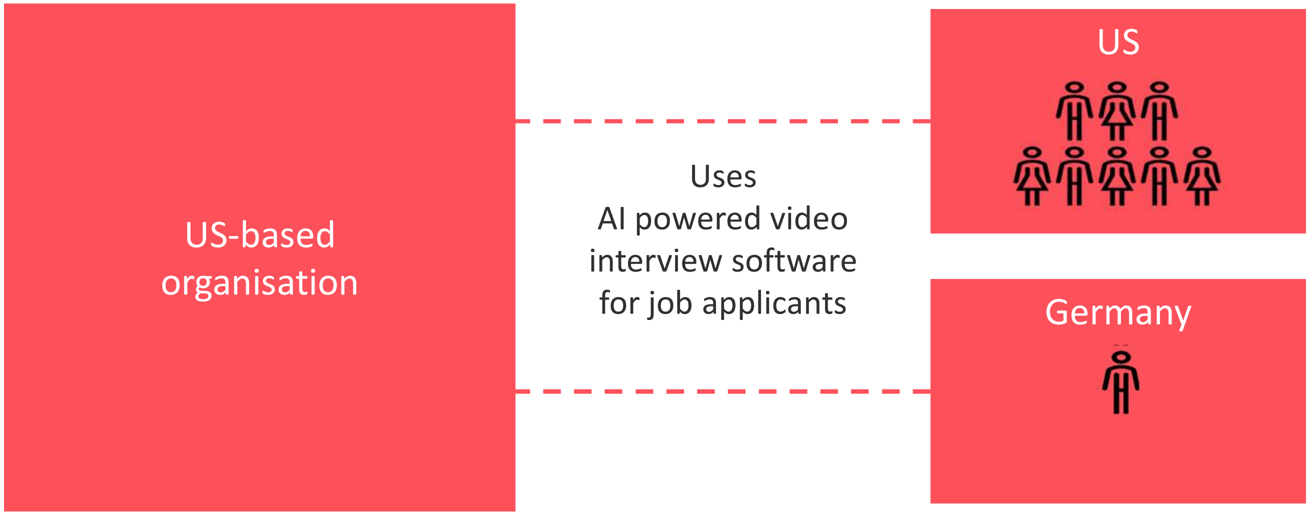
US

Italy

"deployers of AI systems that are established / located outside of the EU, where the output produced by the system is used in the EU"

Article 2(i)(c)

Case study 3: US deployer with EU applicants



US-based organisation

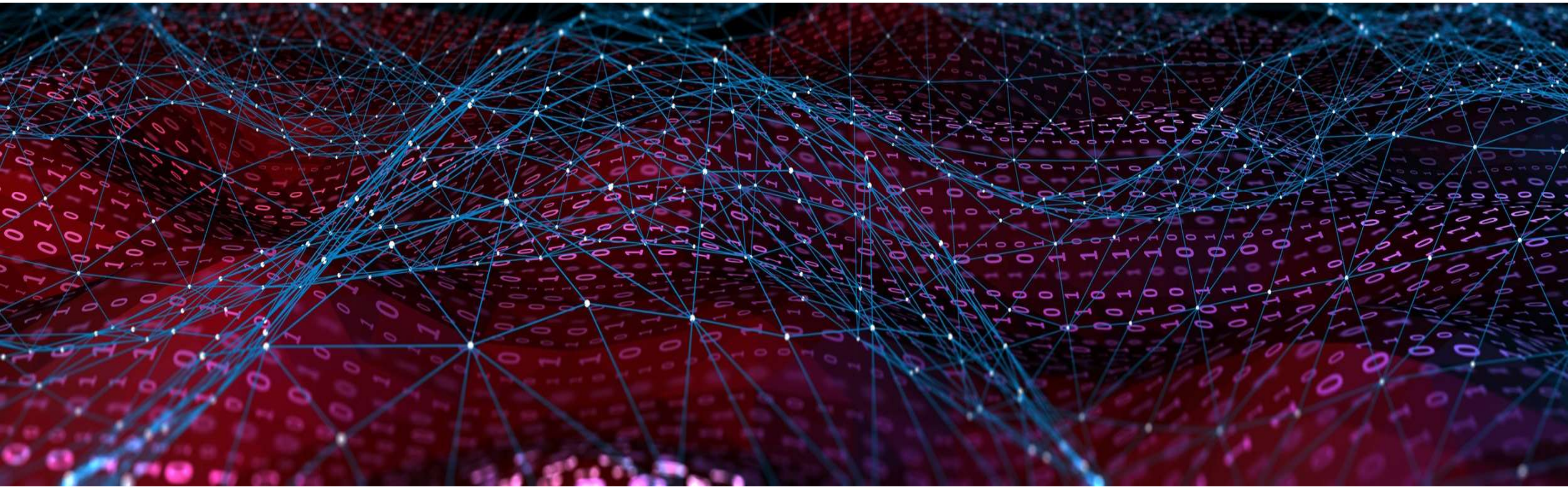
Uses
AI powered video
interview software
for job applicants

US

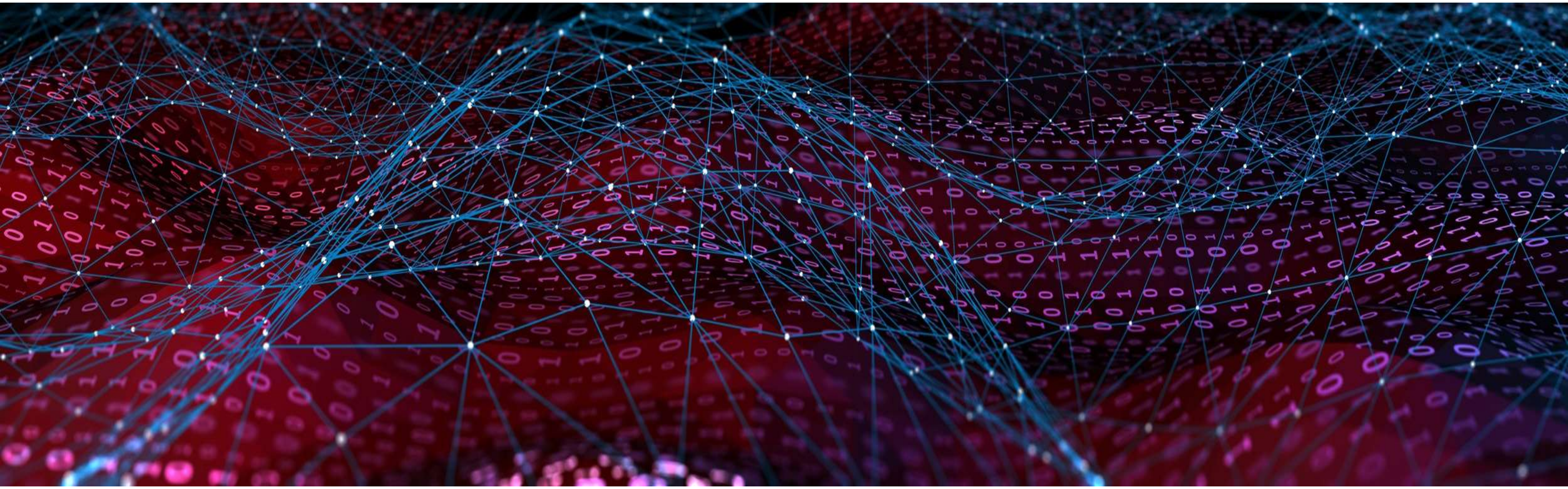
Germany

> "deployers of AI systems that are established / located outside of the EU, where the output produced by the system is used in the EU"
>
> Article 2(i)(c)

AI implementation challenges



Interaction with GDPR



GDPR - Key Considerations

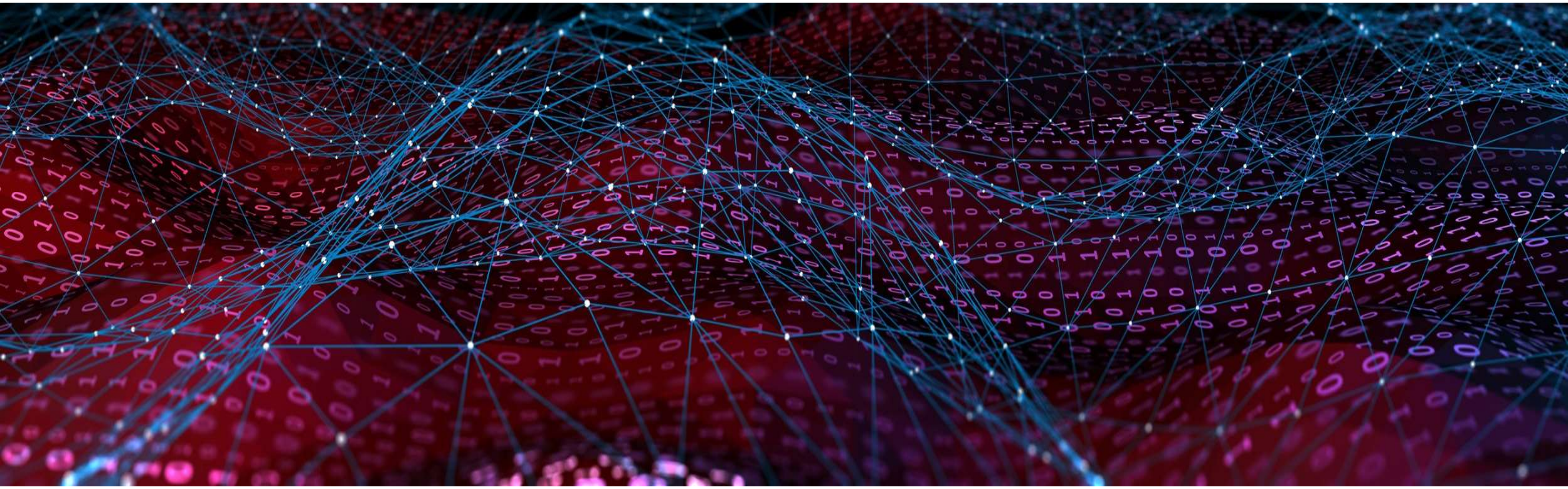
- Scope of **personal data processed** and **applicability** of GDPR
- **Legal basis** for processing (Art. 6 and 9)
- **Transparency** and information provision (Art. 12–14)
- **Automated decision making** and profiling (Art 22)
- **Security** (Art. 32-34):
  - ensuring appropriate levels of security against its unauthorised or unlawful processing, accidental loss, destruction or damage;
  - compliance with breach notification requirements
- **Data privacy impact assessments** (Art. 35)
- Responsibilities and requirements when **using data processors** (Art. 28)

International Data Transfers

International data transfer requirements under the UK GDPR/EU GDPR:

- Transfers of personal data to third countries (i.e. non-UK / EU countries) may only be made when there is a valid legal mechanism legitimizing the transfer.
- Valid legal mechanisms include:
  - ➢ A finding of ***adequacy*** in relation to that third country or international organisation, e.g EU-US Data Protection Framework and UK-US Data Bridge;
  - ➢ ***Standard Contractual Clauses*** (**SCCs**) being agreed between the data exporter and data importer;
  - ➢ ***Binding Corporate Rules*** being approved and implemented; or
  - ➢ Limited ***derogations for specific situations***.
- Where personal data is being transferred between the UK / EU and the US, one of the above mechanisms is required.

Q&A



simmons-simmons.com

Strictly Private and Confidential