Privacy+ Security Forum

TaylorWessing

AI and Data Act

Europe‘s Newest Data Regulation Wave and its impact on US Businesses

10th May 2024 | Dr. Carolin Monsees | Christopher Jeffery | Maeve Ryan

Outline

1.1. AI Act – Overview

Privacy+ Security Forum

TaylorWessing

Overview: „Digital Basic Laws“

Privacy+ Security Forum

GDPR
General Data Protection Regulation

→ Protection of personal data

DGA
Data Governance Act

→ Data sharing infrastructure

DSA
Digital Services Act

→ Creation of a safe digital space free of illegal content

DA
Data Act

→ Access and use of data

EU Digital Basic Laws

DMA
Digital Markets Act

→ Contestable and fair markets of core platform services

AI Act
Artificial Intelligence Act

→ Protection of fundamental rights; support innovation

ePR
ePrivacy Regulation (Draft)

→ Confidentiality of communications; Cookies

AI Act

What is it about?

- First AI regulation worldwide: protection of fundamental rights (health, safety) and support innovation
- “Product Compliance”, market surveillance and monitoring

When?

- Entry into force: adoption expected May or June 2024
- **Applicability mid 2026** (most provisions)

Threat of sanctions?

- Fines of up to 30 million euros or up to 6% of the worldwide annual turnover
- Regulatory restriction or even prohibition of the provision of AI systems

1.2. AI Act – Applicability for US entities

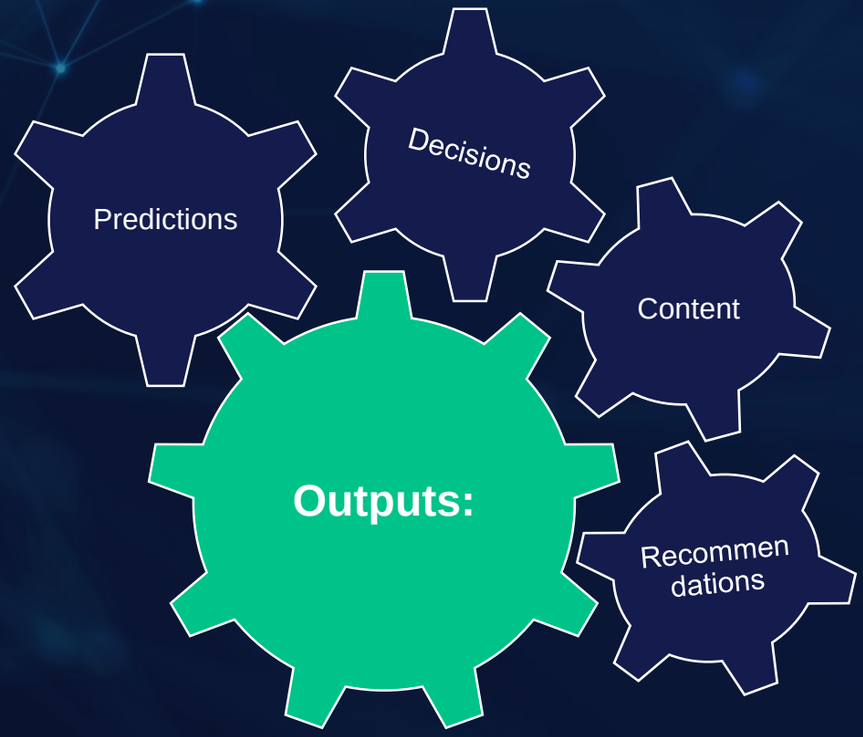
Privacy+ Security Forum

TaylorWessing

Definition of AI Systems

Privacy+ Security Forum

1. **machine-based**
   - with varying levels of autonomy
   - → independent of human control
2. **adaptiveness after deployment**
3. **for explicit or implicit objectives**
4. **infers from inputs**



Corresponds to the definition in EO 14110

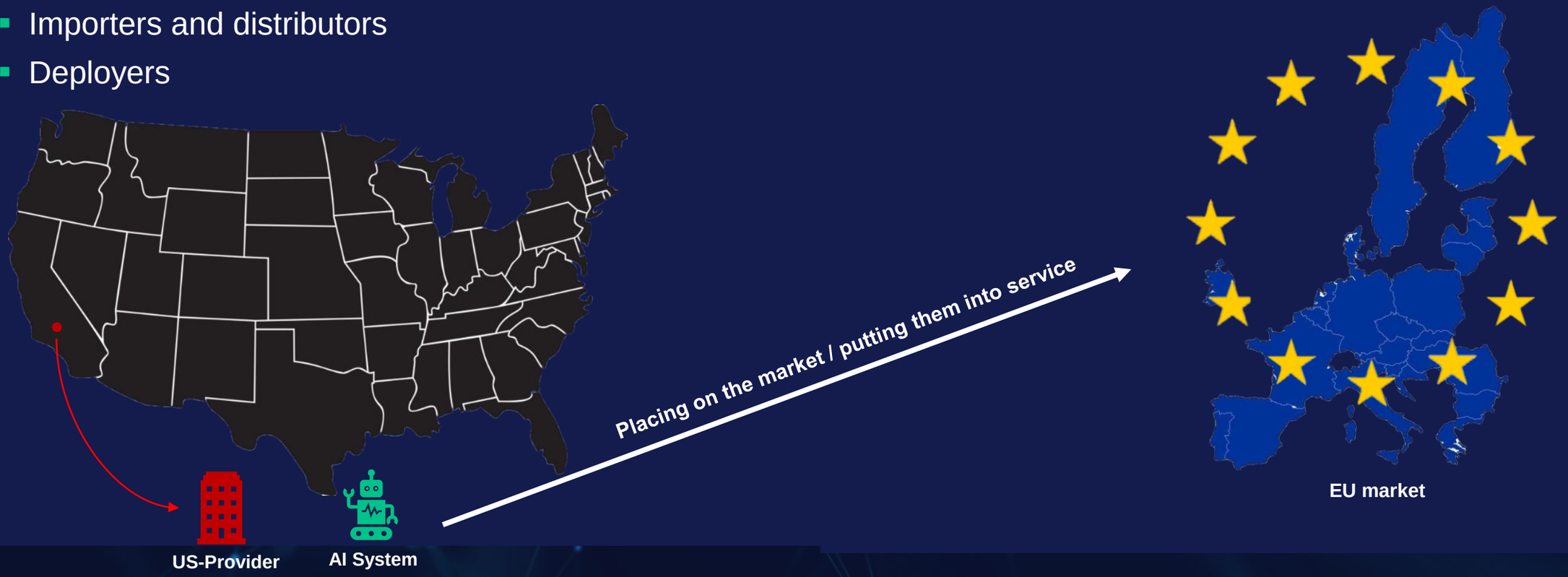
AI Act – Who is affected?

Who is concerned?

- Providers of AI systems
- Importers and distributors
- Deployers

Where does the AI Act apply?

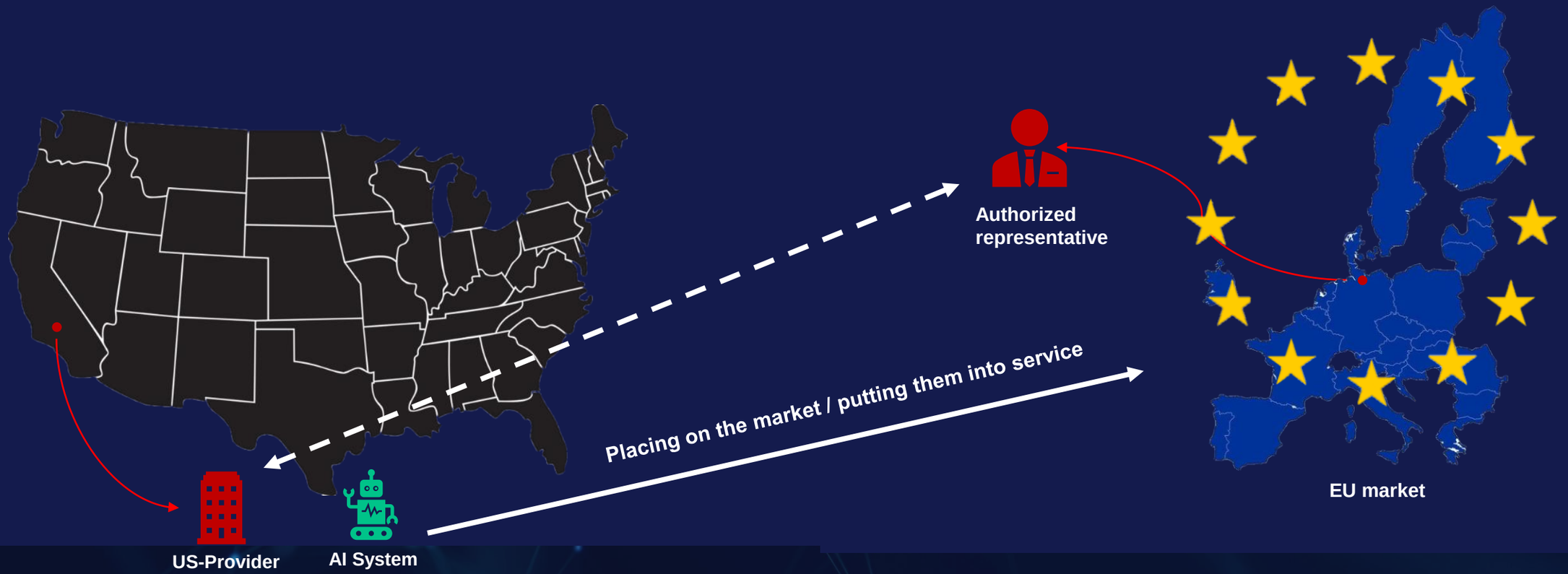
- Extraterritorial approach



AI Act – Who is affected?

Where does the AI Act apply? – Extraterritorial approach

- To US-Providers of AI systems that place their AI system on the EU-market *or* put them into service in the EU



1.3. AI Act – European approach to AI

Privacy+ Security Forum

TaylorWessing

Transatlantic approach to AI

US Approach – Executive Order 14110

- Focuses US companies and the Federal Government
- Needs to be backed by legislative measures to have significant impact (lack of directly prescriptive rules + limited enforceability)
- Binding guidelines; only in residual way resorting to regulation (f.e. generative AI)

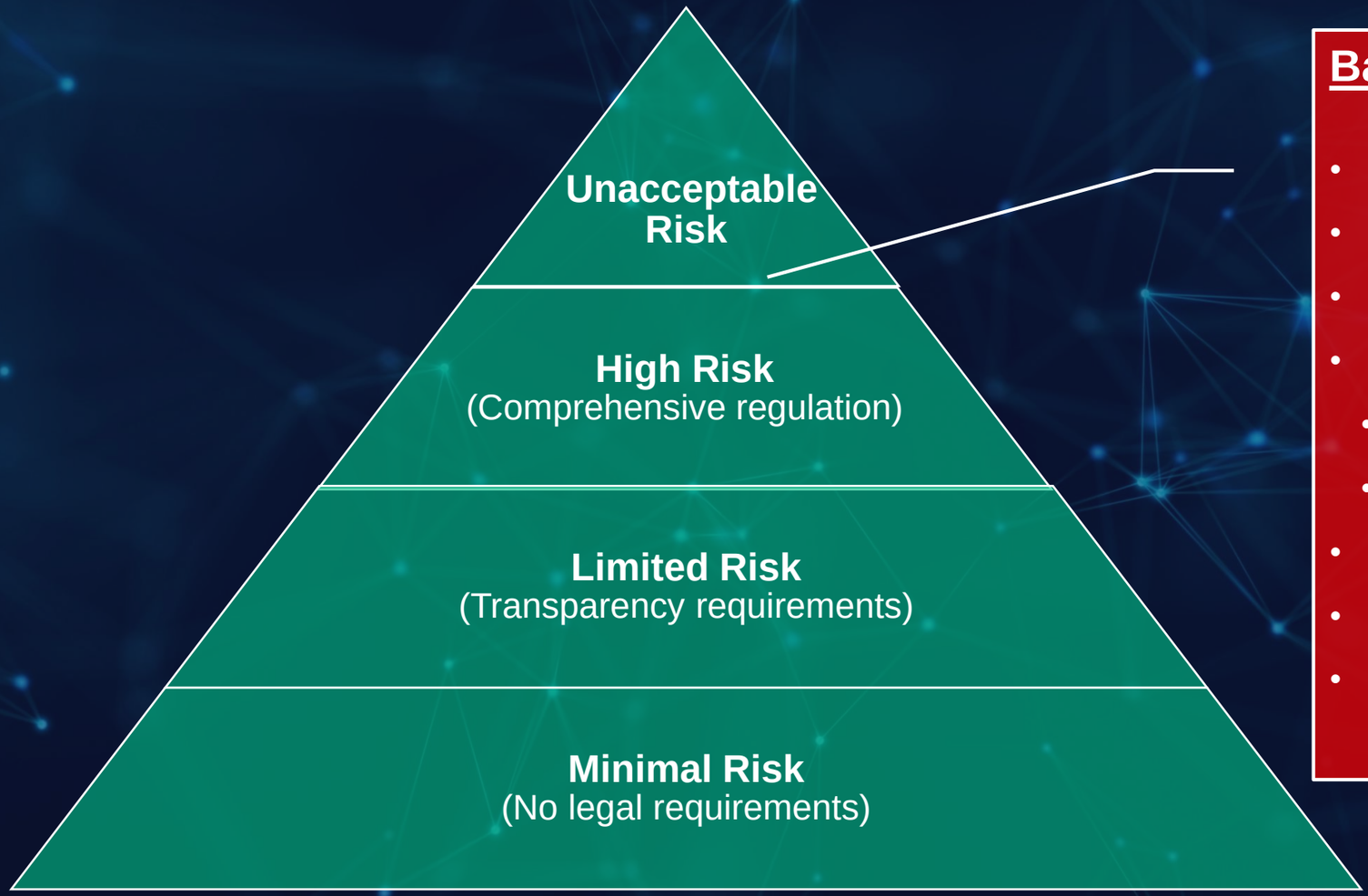
  → regulatory restraint (aim: unleash full potential of AI)

European Approach – AI Act

- Extraterritorial approach (→ may affect US companies)
- EU-wide harmonized direct-acting legal act
- „Risk-based approach“ → categorization of AI systems into different classes of risk
- Comprehensive and detailed set of obligations

  → intended legal certainty (aim: promote innovation)

AI Act – Risk based approach

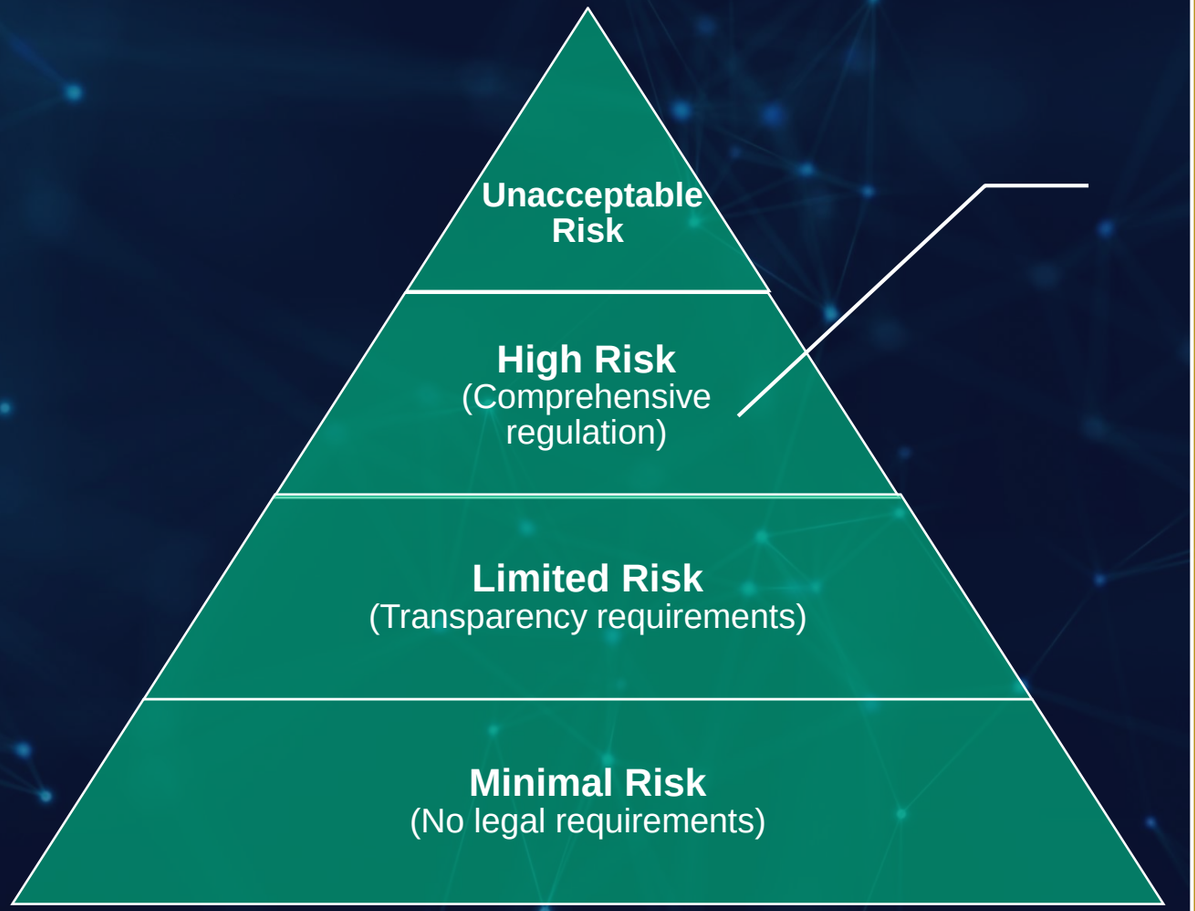


Banned applications:

- **Manipulative AI**
- **Exploitative AI**
- **Social Scoring**
- **Predicitive Policing**
  - Risk assessments
  - Facial recognition databases
- **Emotion recognition (workplace / school)**
- **Biometric categorisation systems**
- **Real time biometric identification systems**

  (but extensive exceptions for law enforcement)

AI Act – Risk based approach



High Risk AI:

Embedded AI

Safety component of a product or the product itself
+
Subject to a conformity assessment

Civil aviation
Recreational craft
Toys
Medical Devices
Agricultural verhicles

listed in Annex I

Non-embedded AI

listed in Annex III

Education and vocational training
Work: Promotion / Termination decisions
Border control
Recruitment
Supply of energy

1.4. AI Act – Requirements and To Do’s

Privacy+ Security Forum

TaylorWessing

AI Act – Requirements

General-purpose AI Models

„Normal“ GPAI models:

- Technical documentation
- Copyright compliance
- Detailed summaries
- Code of practice

High-impact GPAI models (systemic risk):

- Model evaluations & Adversarial testing
- Systemic risk assessment & Cybersecurity measures
- Reporting serious incidents & Energy efficiency reporting

High-risk-AI Systems

- Documentation
- Quality
- Transparency
- Risk management
- Human oversight
- Cybersecurity measures
- Fundamental rights impact assessment
- Conformity assessment

AI Act – To Do‘s I

1. Check: Applicability of AI Act

- Developed Software = AI system / GPAI model or system?
- Scope of application (extraterritorial approach)

2. Risk classification

- GPAI model risk classification
- AI system risk classification

3. Preparation for regulatory actor-specific obligations

- Provider / Deployer?
- Conformity assessment (Compliance with AI requirements)
- Appointment authorized representative

4. Market Launch & post-market surveillance

- CE-Declaration
- Post-market surveillance as required
- Recertification in the event of significant deviations

Don‘t forget GDPR

AI Act – To Do's II

Relationship with Responsible AI governance

- **Apply the programme!**

What help will we get?

- Codes of practice expected
  - GPAI models within 9 months
  - maybe others – timing unclear
- AI Board may issue guidance on technical specifications or existing standards re high-risk systems
- 18 months – so end of 2025: AI board to publish guidelines incl comprehensive list of practical examples of use cases of AI systems that are high-risk and not high-risk. With 6 months to go!
- Range of secondary legislation enabled, but no timing set
- Do the categorisation analysis and build the essentials of AI compliance flying blind

Some specific bear-traps

- Watch straying into provider compliance:
  - Deployers making substantial changes to a high-risk system already on the market (art 25)
  - Deployers modify the intended purpose of an AI system which is not high risk so it becomes high-risk

Potential out for high-risk systems?

- Narrow procedural tasks
- Improve result of human activity
- Decision-making patterns
- Tasks preparatory to an assessment

High-risk compliance – what tools are there?

- Eventually, Commission/ AI Office may help
- AI Act assigned standard-setting to CEN and CENELEC – timing unclear
- Use NIST AI RMF or ISO/IEC 42001:2023 AI management system?

1.5. AI Act – Interpretation and implementation

Privacy+ Security Forum

TaylorWessing

Interpretation

Definitions evolved over time

Commission - 2021

‘artificial intelligence system’ (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; Annex 1 referred to machine learning, as well as logic and knowledge based approaches, statistical approaches and search and optimisation methods.

IMCO/LIBE (Parliament) - June '23

‘‘artificial intelligence system’ (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;

Final text – Jan '24

‘AI system’ means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;

Planning for implementation

Interpretation

- Had do to assess the feasibility of potential requirements for systems as they might be in 2024/2025 when the AI Act would be enforceable
- Required input from a cross-functional (XFN) team, with deep technical and broad institutional knowledge
- Had to estimate the potential impact of implementation amidst uncertainty about where the text would end up, how technology will have evolved etc.

To implementation

- As the AI Act has been evolving, so has our own internal AI governance – due to both internal and external factors e.g.:
  - Open source approach
  - Cross-industry efforts like PAI, ML Commons
  - Regulatory effects
- Our governance needs to map across regulation inc. the AI Act, industry frameworks, and internal needs. Large XFN effort

2.1. Data Act – Overview

TaylorWessing

Data Act

What is it about?

Promoting availability and usability of data (personal and non-personal) in the EU through

- Rights of access to and use of data
- Interoperability of data + easy cloud switching
- Obligation to make data available in exceptional cases (B2G)

When?

- Entry into force: 11. January 2024
- Applicability 12. September 2025

What actions must be taken?

- Contract / T&C amendments
- Technical adaptations
- Organizational adjustments

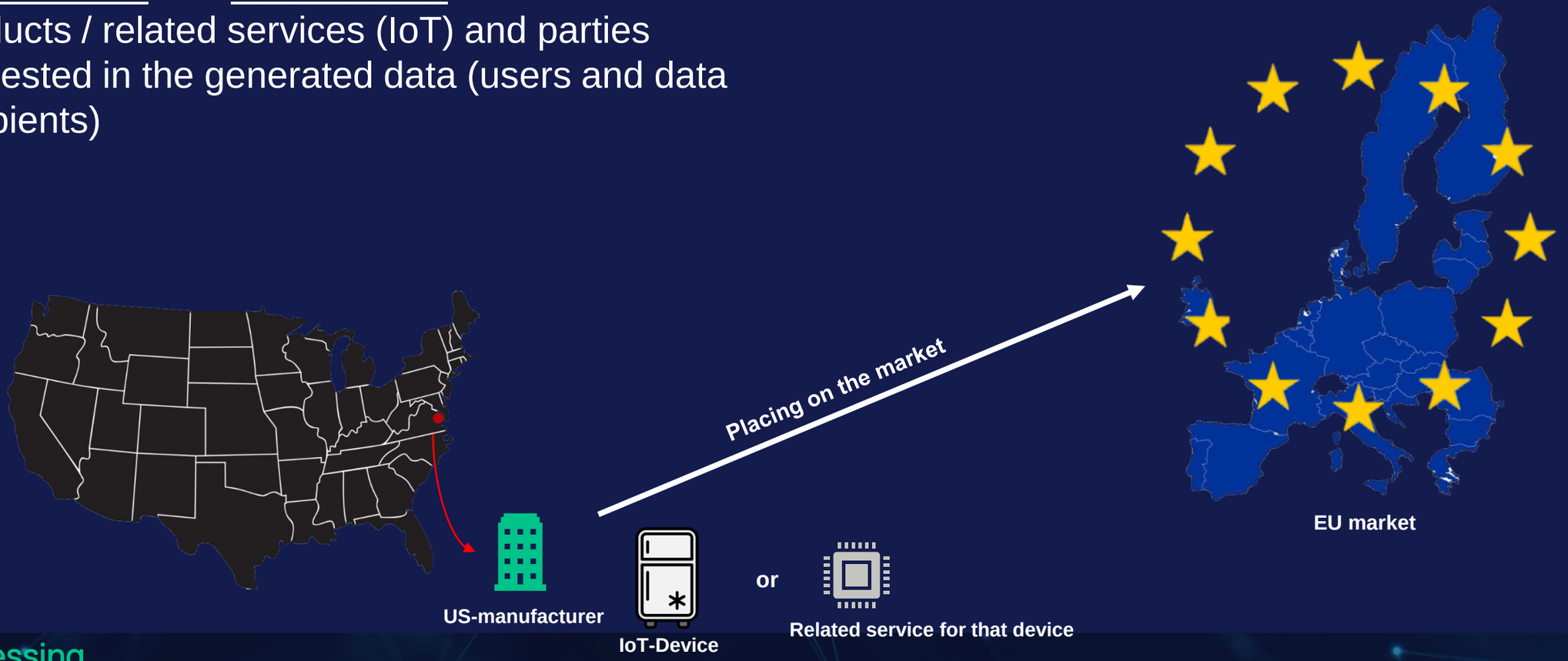
Threat of sanctions?

- Fines of up to 20 million euros or up to 4% of the worldwide annual turnover (reference to GDRP)

Data Act – Who is affected?

Who is concerned?

- Manufacturer and data holders of connected products / related services (IoT) and parties interested in the generated data (users and data recipients)



2.2. Data Act – Connected products & cloud switching

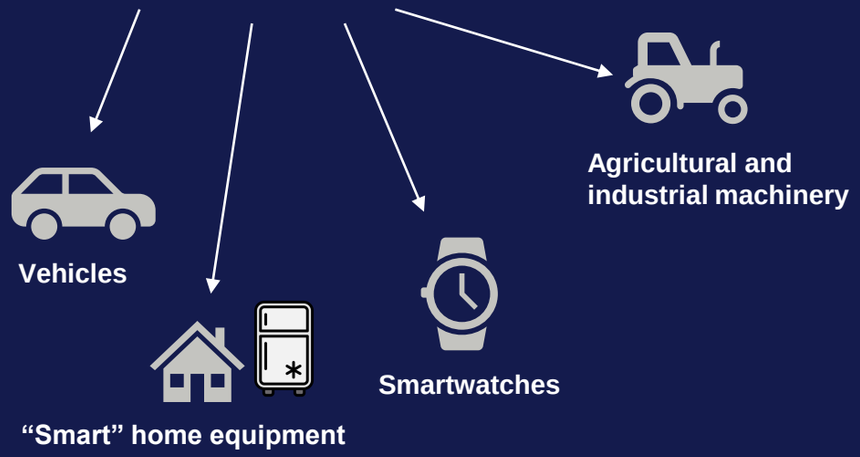
Privacy+ Security Forum

TaylorWessing

Data Act – Connceted products

Connected products

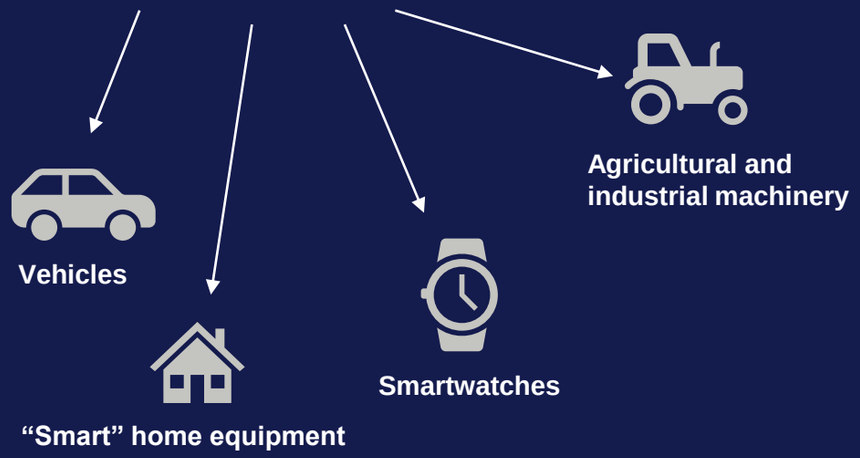
- Generate / collect data concerning its use or environment
- Communicates the data
- Primary function is not the storing, processing or transmission of data



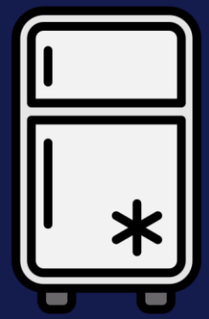
Data Act – Connceted products

Connected products

- Generate / collect data concerning its use or environment
- Communicates the data
- Primary function is not the storing, processing or transmission of data



Example: IoT Fridge

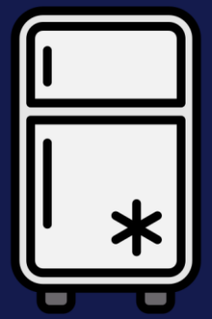


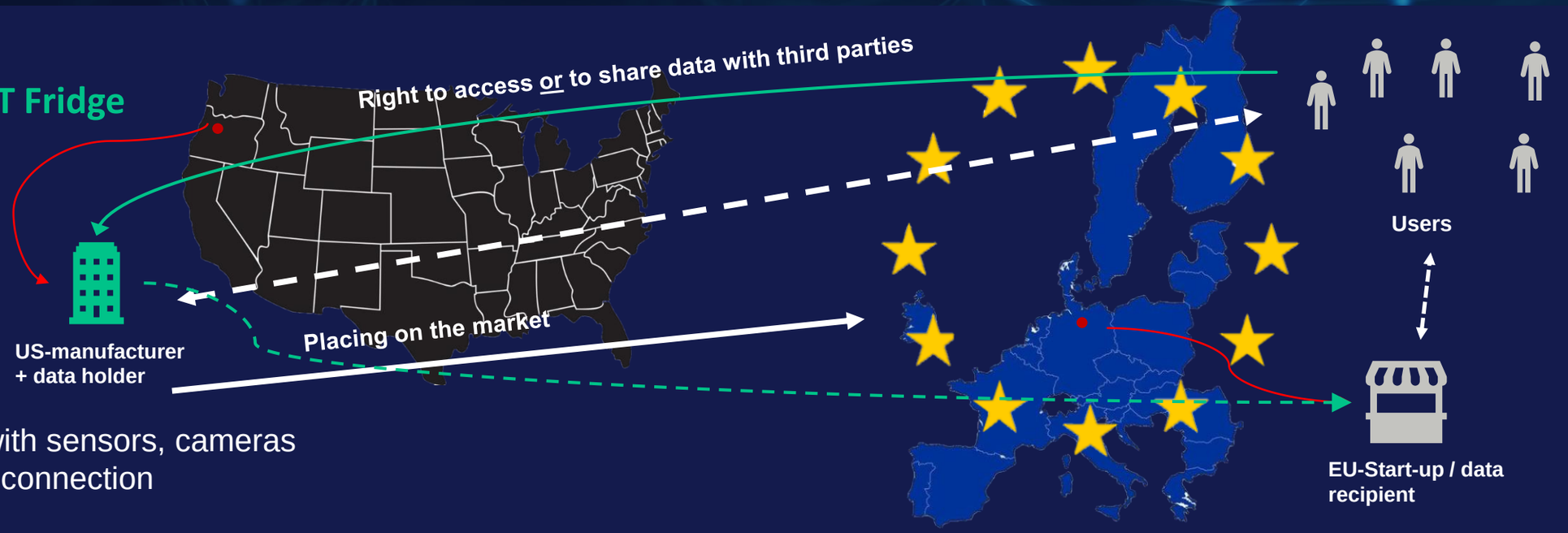
- Equipped with sensors, cameras and WLAN connection

→ Collects data of **temperature** on different levels

Data Act – Data access

Example: IoT Fridge





- Equipped with sensors, cameras and WLAN connection

  → Collects data of **temperature** on different levels

- Goal: develop related service

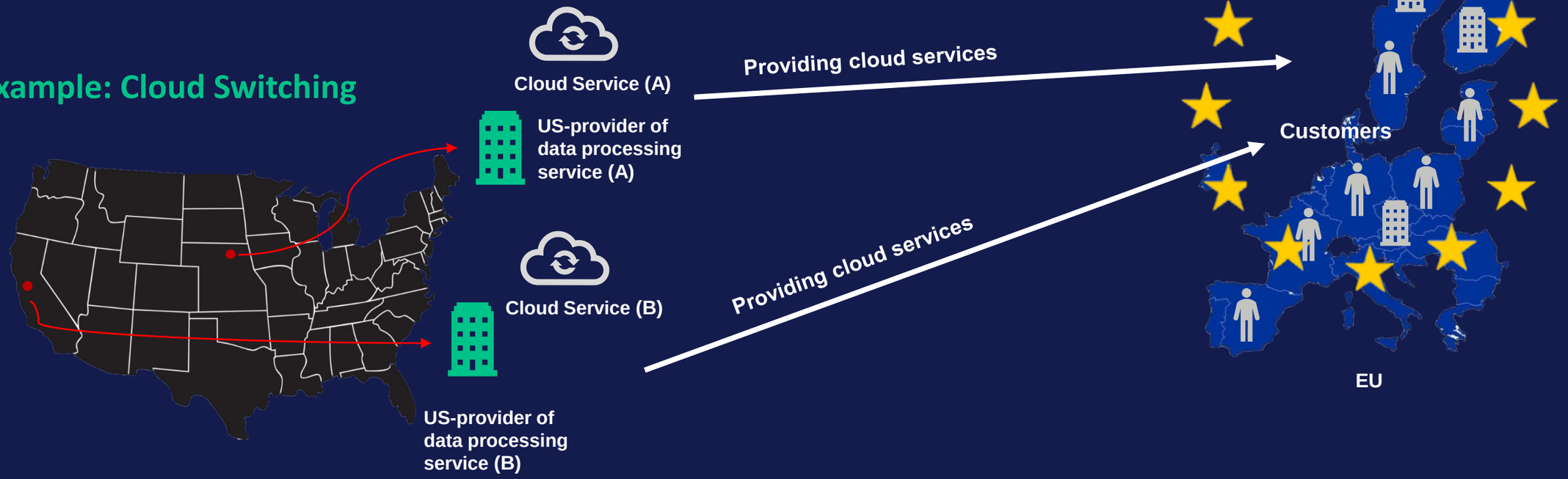
  → better temperature regulation (thus, improved energy efficiency)

Data Act – Cloud switching

Data processing services

- Digital service → enables ubiquitous and on-demand network access to a shared pool of computing resources
- In practice: f.e. IaaS, PaaS, SaaS, Storage-as-a-Service or Database-as-a-Service

Example: Cloud Switching

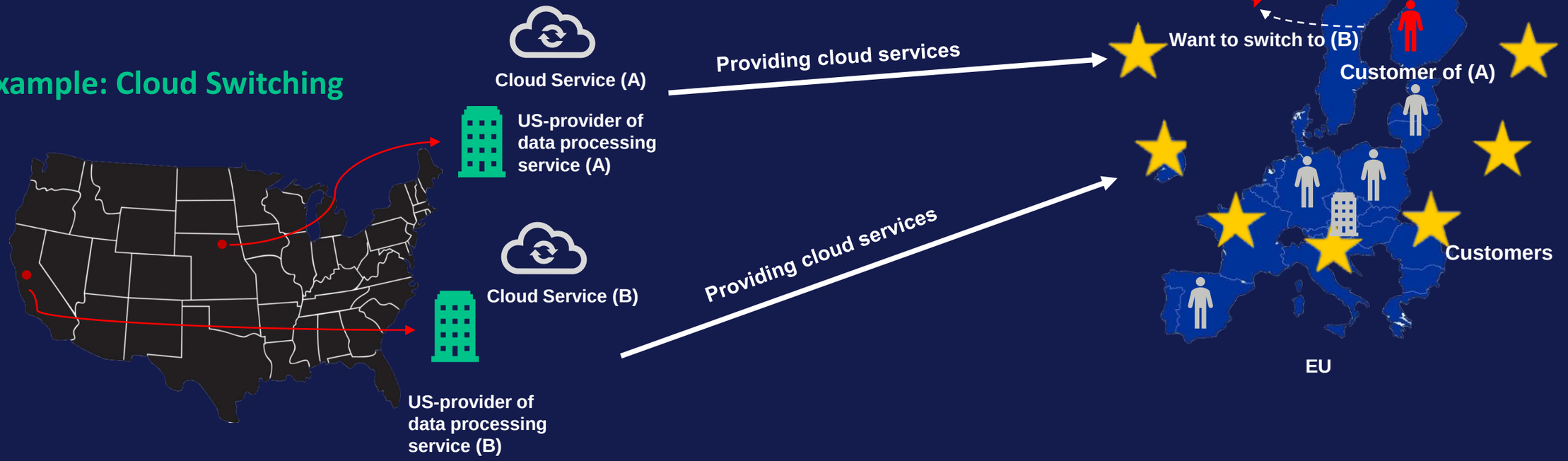


Data Act – Cloud switching

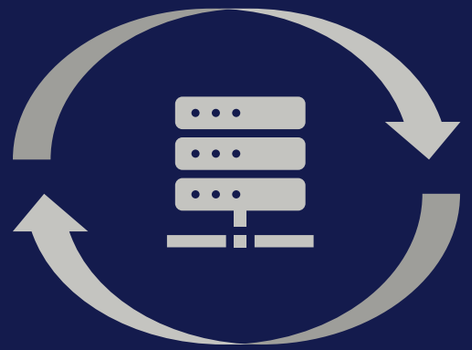
Data processing services

- Digital service → enables ubiquitous and on-demand network access to a shared pool of computing resources
- In practice: f.e. IaaS, PaaS, SaaS, Storage-as-a-Service or Database-as-a-Service

Example: Cloud Switching



Cloud switching – Requirements



Aim: switching between data processing services

- Removal of
  - Lock-in effect
  - Vendor-lock-in effect
- Promotion of competition

Requirements for providers

- Contract/T&C amendment (right of customer to switch)
- Removing obstacles to effective switching
- Information obligation
- Transparency
- Gradual withdrawal of switching charges
  - 11. January 2024 → 12. January 2027: reduced charges
  - From 12. January 2027: no charges
- Implementation of interoperability standards

2.3. Data Act – To Do’s

Privacy+ Security Forum

TaylorWessing

Data Act – To Do‘s

1. Check: Applicability Data Act

- Manufacturer or data holder of IoT-device?
  → device a connected product / related service?
- Data processing service (Cloud-service)?

2a. Data processing service

- Contract/T&C amendment
- Implementation of interoperability standards
- Check further guidance

2b. IoT

- Contract/T&C amendment
- Technical adaptions (data accessibility by design; smart contracts; interoperability)
- Compliance management
- Defense strategy against data access requests
  → preparation: identification of trade secrets

Don‘t forget GDPR

Privacy+ Security Forum

3. The Speakers

TaylorWessing

Speakers

Privacy+ Security Forum

Dr. Carolin Monsees
Salary Partner,
Taylor Wessing

Christopher Jeffery
Partner,
Taylor Wessing

Maeve Ryan
AI Policy Manager,
Meta

TaylorWessing