Data Protection & Privacy in a Geopolitical World

Content

1. Geopolitics - background
2. EU Digital Strategy
3. Overview of key legislative initiatives
4. Capabilities to manage complexity
5. Conclusions

Geopolitics - background

Geopolitics in a digital world

Digital Strategic Autonomy - Control of Infrastructure and Data

- Industrial Policy
- Innovation Policy
- Foreign Policy
- National Security Policy
- Protecting Citizens
- Protecting Companies
- Protecting the constitutions

- Technology leadership
- Protection of infrastructure
- Technology standards
- Legal and regulatory standards
- Shaping new markets and opportunities
- Supply chain risk management
- Ability to enforce your own laws

Geopolitical shifts with significant disruptive effect

US/China strategic competition

- Trade restrictions
- Divergence in standards
- Restrictions on certain industries

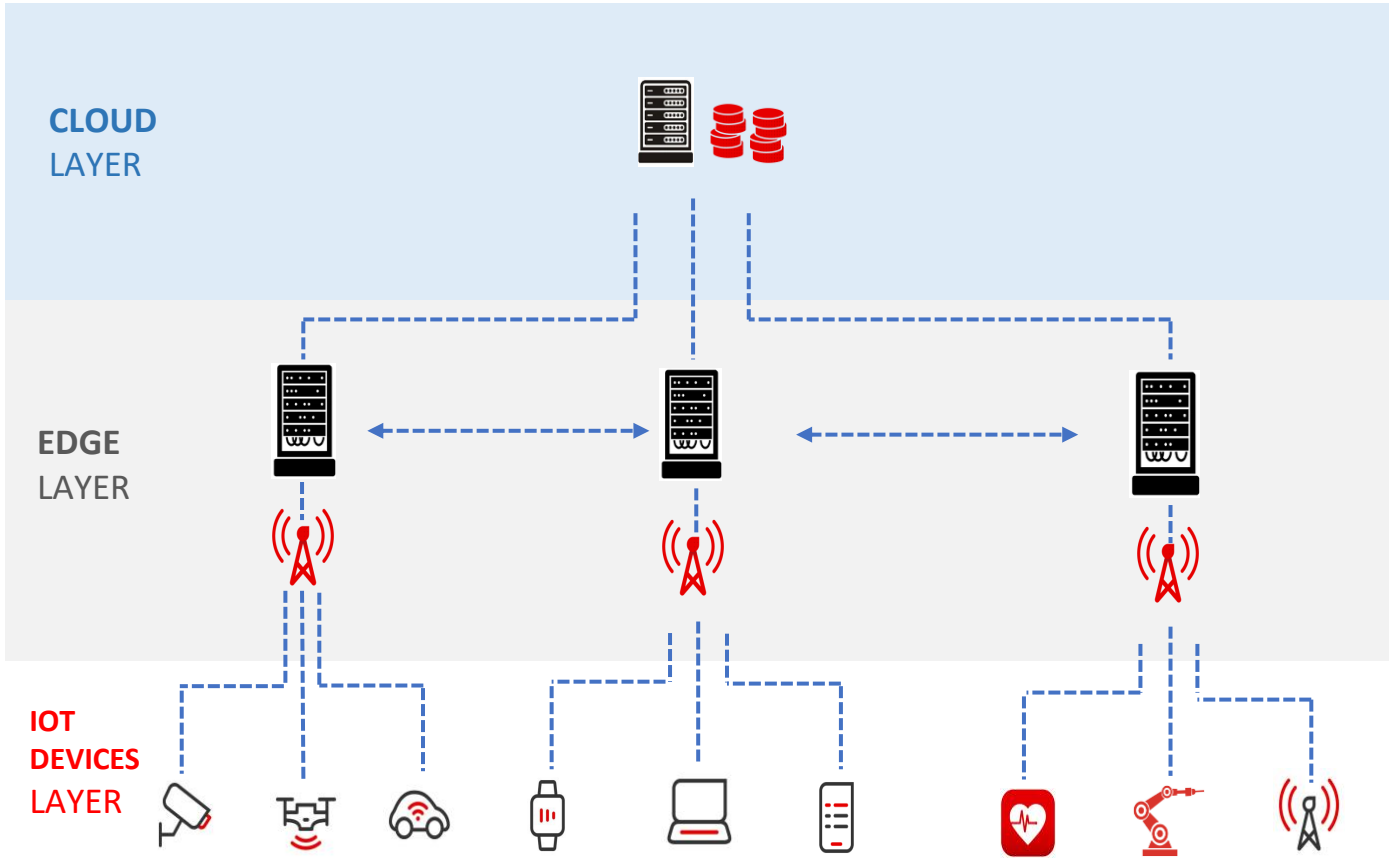
From globalisation to nationalistic policies

- Data localisation
- Supply chain
- Barriers to large-scale investments

Increase focus on national security, autonomy, re-shoring, tech sovereignty and resilience

EU Digital Strategy

European Cloud Market?



- ✓From €53bn in 2020 to €560bn by 2030
- ✓Low level of cloud adoption in Europe
- ✓Massive data volume increase
- ✓69% of European cloud services with hyperscalers

1. “Globalised Free Market”?
2. “Fortress Europe”?
3. “Open Strategic Sovereignty”?

Digital Sovereignty – EU Data Strategy

European Digital Single market

WHY?
- Volume and importance of data increasing
- European competitiveness
- Climate, health, transport & other policy objects

ISSUES?
- Fragmentation
- Availability of data
- Big Tech, US & China dominance
- Unclear rules on data rights
- Competence gaps
- Foreign access
- Misinformation & manipulation

VISION?

European Way
- Data flows freely in Europe
- Data follows European rules and values
- Fair rules & interoperability
- Trusted & governed
- Cyber security
- Privacy & data protection
- Controlled international transfers
- Skills & competences

Digital Sovereignty – EU Data Strategy

Common European Data Spaces – Pooling data from key sectors

Health	Industrial	Agriculture	Finance	Mobility	Green Deal	Energy	Public Administration	Skills

Marketplace for Cloud Edge based services – AI

Rich pool of data
Privacy & Data Protection
Free flow of data across sectors and countries
Horizontal framework for data access and governance

Overview of key legislative initiatives

Digital Sovereignty – EU Data Strategy

Creating a digital single market – legislative package

DMA	DSA	DGA	DA	AI	CRA
Digital Markets Act	**Digital Services Act**	**Data Governance Act**	**Data Act**	**Artificial Intelligence Act**	**Cyber Resilience Act**
May 2023	*May 2023*	*Sept 2023*	*N/A*	*N/A*	*N/A*

GDPR, ePrivacy, Free Flow of Data
Cyber Security Strategy (NIS2, 5G Security Toolbox etc.)

Digital Markets Act

Competitive and fair digital sector

Applies to

- Core platform services, designated gate keepers (very large platforms with >45m monthly users/10k business users or €75m market cap / last 3 years)

Sets requirements, e.g.

- No cross-use / combining of personal data
- No automatic sign-up of users to other services
- No use of personal data relating to users of third party services on the platform for advertising
- No use of business users' data to compete with them
- Access to and effective portability of data
- Access to 3rd party search engines to ranking, query, click and view data

Effective

- May 2023, designation of gatekeepers mid-2023 and compliance in 2024.

Fines

- up to 10% of global turnover, and 20% for repeat infringements

Digital Services Act

Combat illegal content, increase transparency, improve accountability, manage systemic risk

Increasing obligations per intermediary service's role, size and impact

- Network infrastructure
- Hosting
- Online platforms
- Very large online platforms (>45m users)

Obligations include e.g.

- Changes in intermediary liability (e.g. reporting of serious crimes)
- Notice and action (hosting)
- Co-operation with regulators
- Trusted flaggers for illegal content
- Transparency reporting, complaint handling on content decisions
- Verification of traders in online market-places
- Recommenders without profiling
- Risk assessment for systemic risks

Effective

- May 2023, designation of gatekeepers mid-2023 and compliance in 2024.

Fines

- Up to 10% of global turnover, and 20% for repeat infringements

Data Governance Act

Increase trust and facilitate data sharing

Applies to

- Public sector bodies
- Data intermediation services
- Data altruisms organisations

Sets up a governance framework for data accessibility

- Conditions for re-use of public sector data
- Notification & supervisory framework for data intermediation services
- Voluntary registration for data altruism organisations

International transfers restrictions

Effective: September 23rd, 2023

Fines: Member state discretion

Data Act

Make data available and fairness

Applies to

- Manufacturers of IoT/IoB & suppliers of related services
- Data holders & Data recipients
- Data processing services (cloud & edge)

Sets rules on

- Rights to access and use data & transparency
- Making private data accessible to public sector in exceptional circumstances
- Remove barriers of switching
- Interoperability)

International transfers restrictions

Effective N/A

Fines 4% of annual global turnover

AI Act

Manage AI risks through controls and transparency

Applies to

- AI systems & providers
- Importers & Distributors
- Users

Sets rules on

- Prohibited AI
- High Risk AI
- Limited Risk AI
- Minimal Risk AI

Effective:

- N/A (earliest 2024 - 2nd half)

Fines:

- €30m or up to 6% annual global turnover (prohibited AI)
- €20m or up to 4% annual global turnover (other AI)

AI Act

AI Act

Prohibited AI

clear threat to safety, livelihoods and rights of people

- Subliminal manipulation
- Facial Recognition in public spaces
- Exploit people's vulnerabilities (e.g. age, disabilities)

High Risk AI

- Biometric identification & classification
- Critical infra management
- Education
- Employment
- Access to essential services
- Law Enforcement (e.g. risk assessment, profiling, evidence evaluation)
- Migration, asylum, border control
- Justice

Requirements, e.g.

- Risk Management System
- Quality of Training, Validation & Test data
- Quality Management System
- Technical documentation
- Logging
- Human oversight ("stop")
- Accuracy
- Instructions to users
- Cyber security (incl. integrity attacks)
- Conformity assessment & registration & CE mark
- Transparency for human facing AI & Deep fake tag

Cyber Resilience Act

Improve security of products with digital elements

Applies to very broad range of digital products

- Operating systems, device management
- Browsers, Routers, IoT devices, Apps
- Network management tools
- Identity management, firewalls etc.
- Industrial Automation systems etc

Requirements, e.g.

- Secure by Design
- Data minimisation (inc. non-personal data)
- Confidentiality, Integrity, Availability, Resilience
- Vulnerability handling, testing, updateability
- Responsible disclosure
- Transparency of security posture

Conformity

- CE mark

Effective:

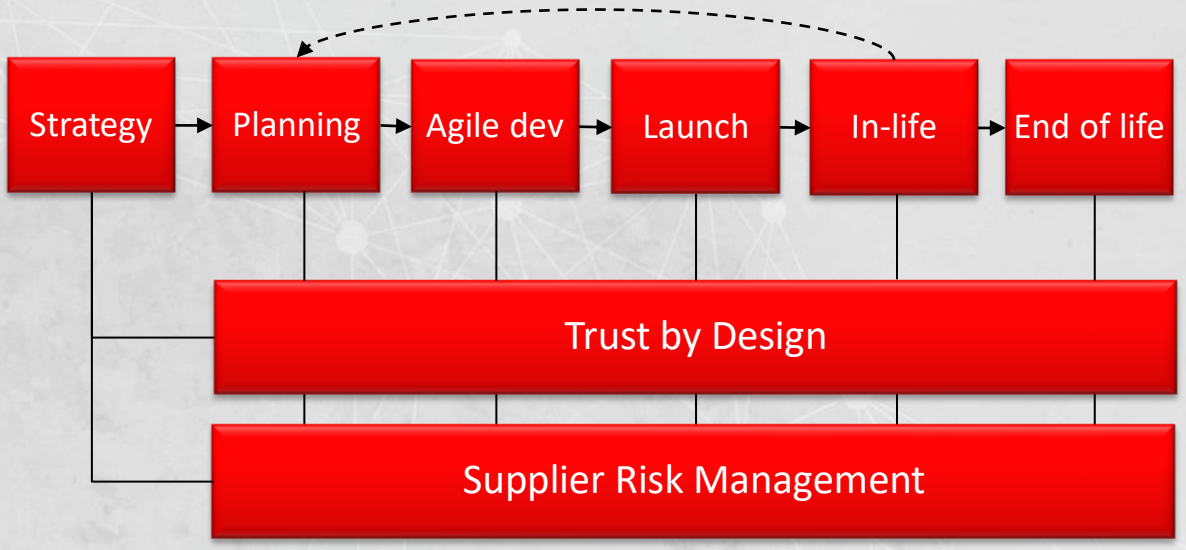
- N/A

Fines:

- €15m or up to 2.5% global annual turnover

Capabilities to manage complexity

Trust by Design - process

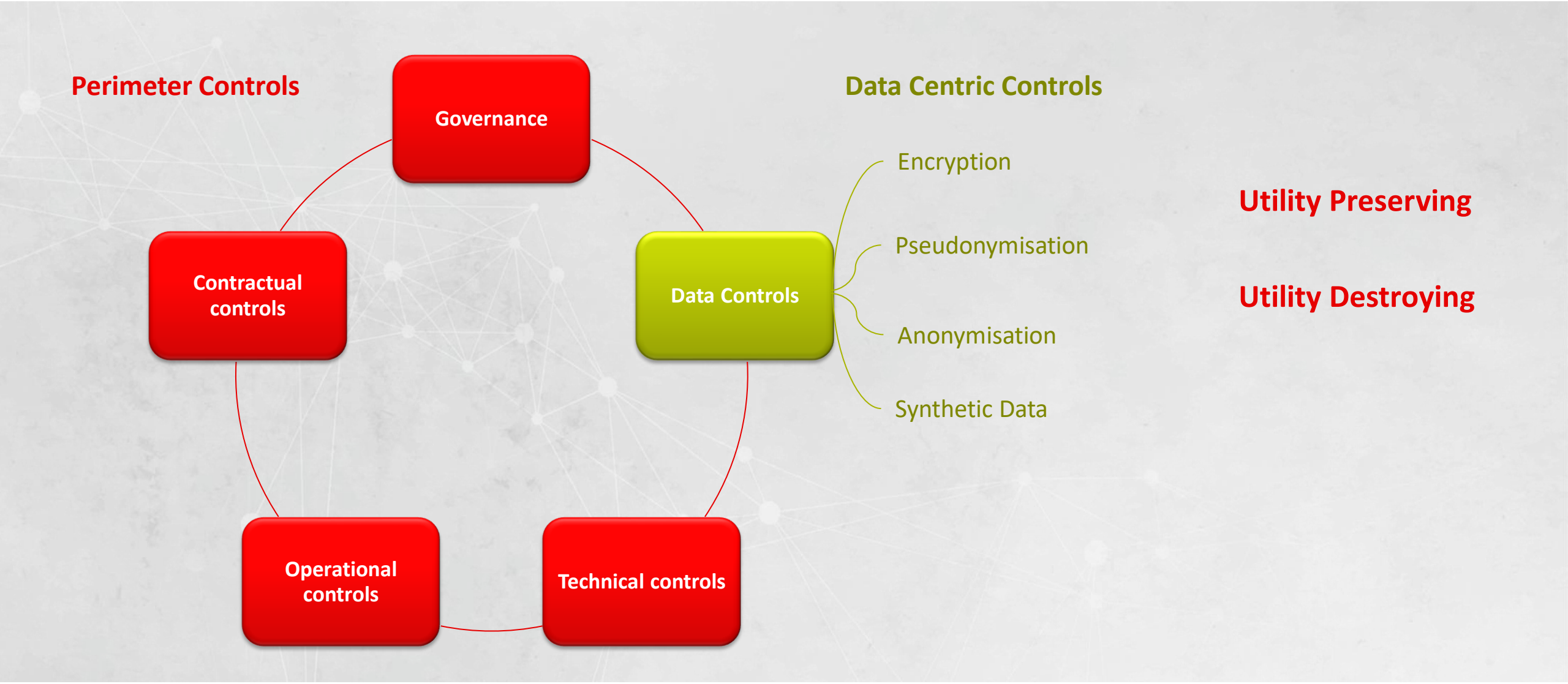


Policies, standards, processes, people, training, monitoring

Trust by Design

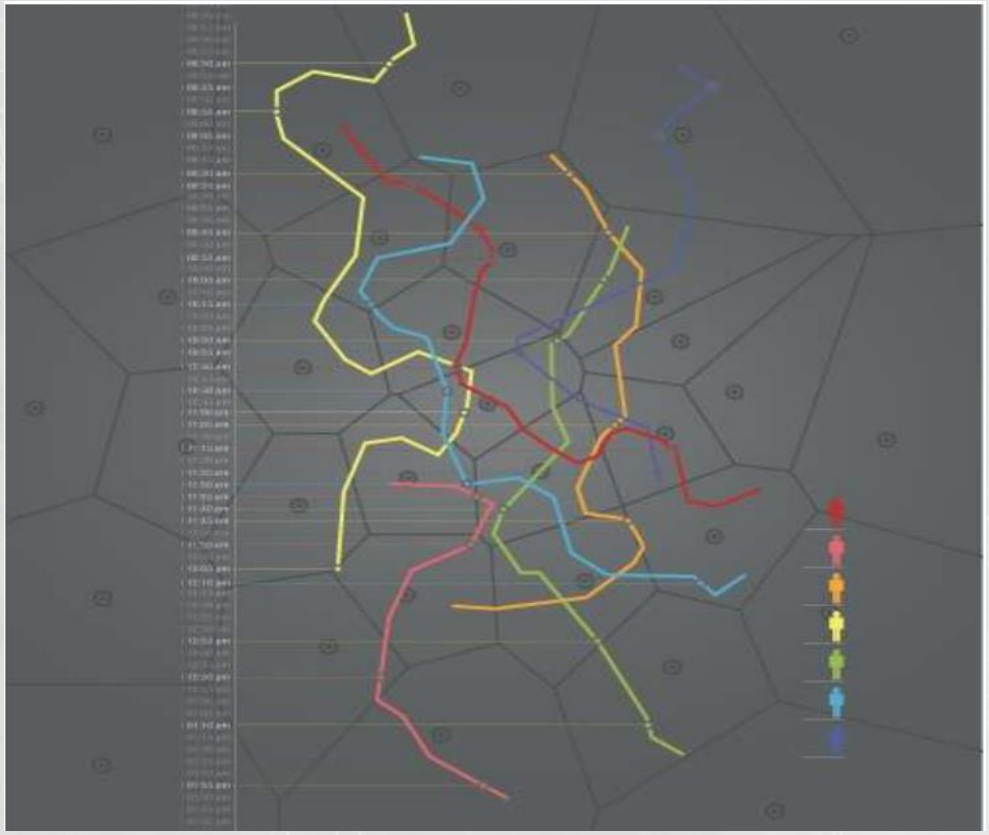
- Data by Design
- Privacy by Design
- Secure by Design
- Responsible AI by Design
- Trade & Sanctions by Design
- Human Impact Assessment
- Transfer Impact Assessment
- Supply Chain Compliance
- Engineering & Architecture

Data Centric Controls



Anonymisation of mobile data is not easy

Cell-ID + time stamp + Anonymous Unique Persistent User ID = easily not anonymous



Anonymised and aggregated to high level (>15) + large enough regional area (e.g. NUTS3) = anonymous

Human Impact Assessment

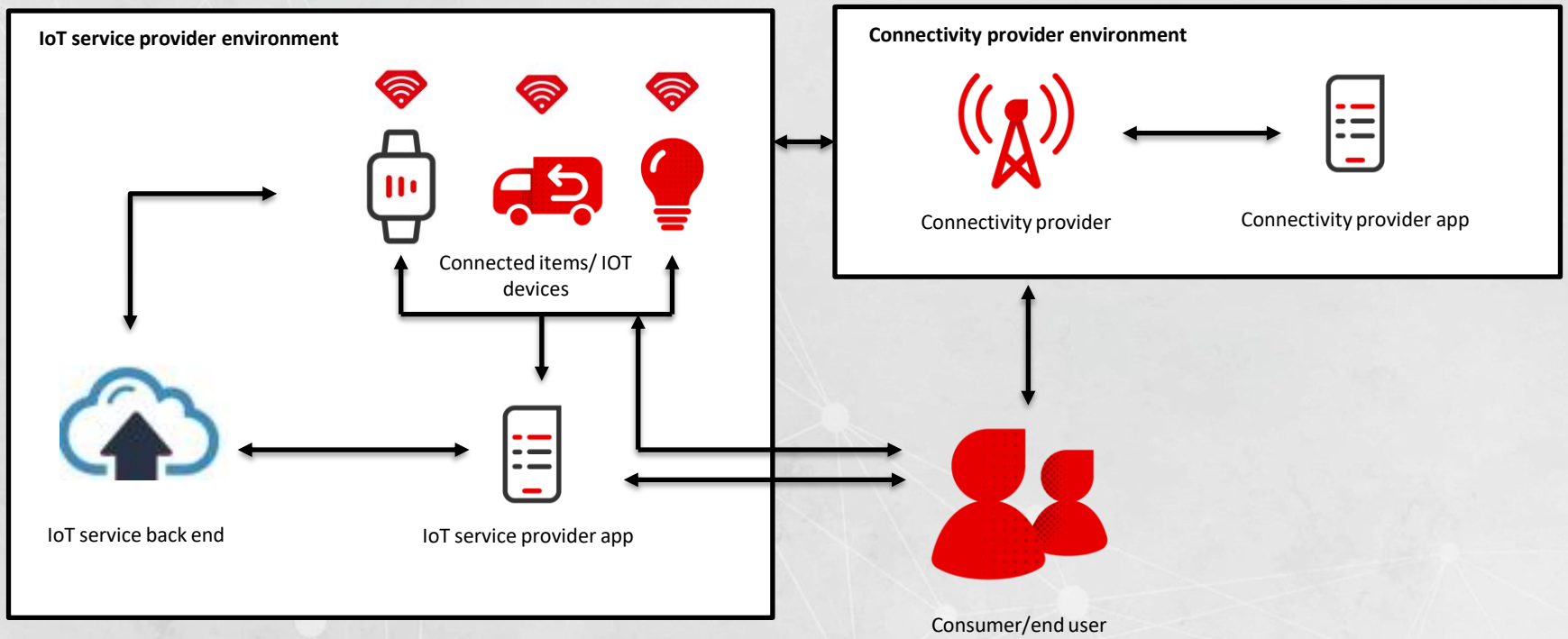
Tangible

1. Death
2. Bodily Harm
3. Loss of freedom of movement
4. Property / asset harms
5. Monetary loss / fraud
6. Blocked or differential access to credit
7. Negative impact on employment
8. Loss of services

Intangible

1. Damage to reputation, embarrassment
2. Emotional distress
3. Nuisance, irritation
4. Verbal abuse
5. Loss of sense of personal security
6. Loss of control over one's personality
7. Inability to exercise privacy or other rights
8. Loss of freedom of movement
9. Loss of freedom of association
10. Loss of freedom of political opinion, religious beliefs
11. Bias, stereotyping, unlawful discrimination
12. Loss of opportunity
13. Loss of control over the purposes of processing of personal data

Ecosystem thinking – IoT as an example



Conclusions

Conclusions

Geopolitics is here to stay

Europe wants to find a European Way

- Build strategic autonomy
- Create fair, safe and secure online and digital infrastructure and services
- Make more data available and interoperable
- Increase transparency
- Prevent foreign access to data
- Prevent cyber threats
- Prevent supply chain risk
- Manage algorithmic, AI & misinformation risk
- Protect privacy, copyrights, other rights

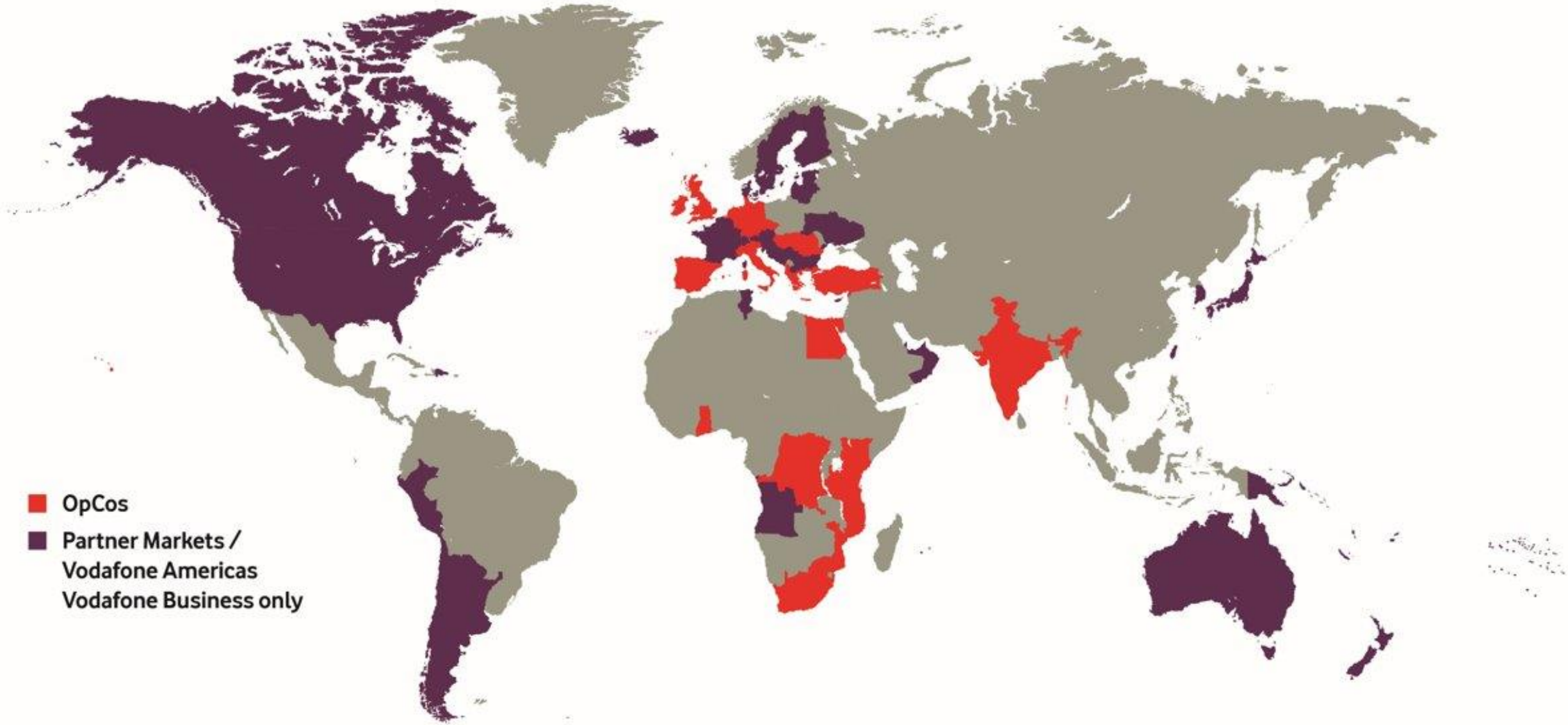
Heavily sanctioned

Organisational capabilities are key

Questions?

Vodafone operations and partners

September 2022



Digital Sovereignty – EU Data Strategy

Common European data space - creating a digital single market

Phase 1 2010-2020

Promote Growth & Fair, Open and Secure Digital environment

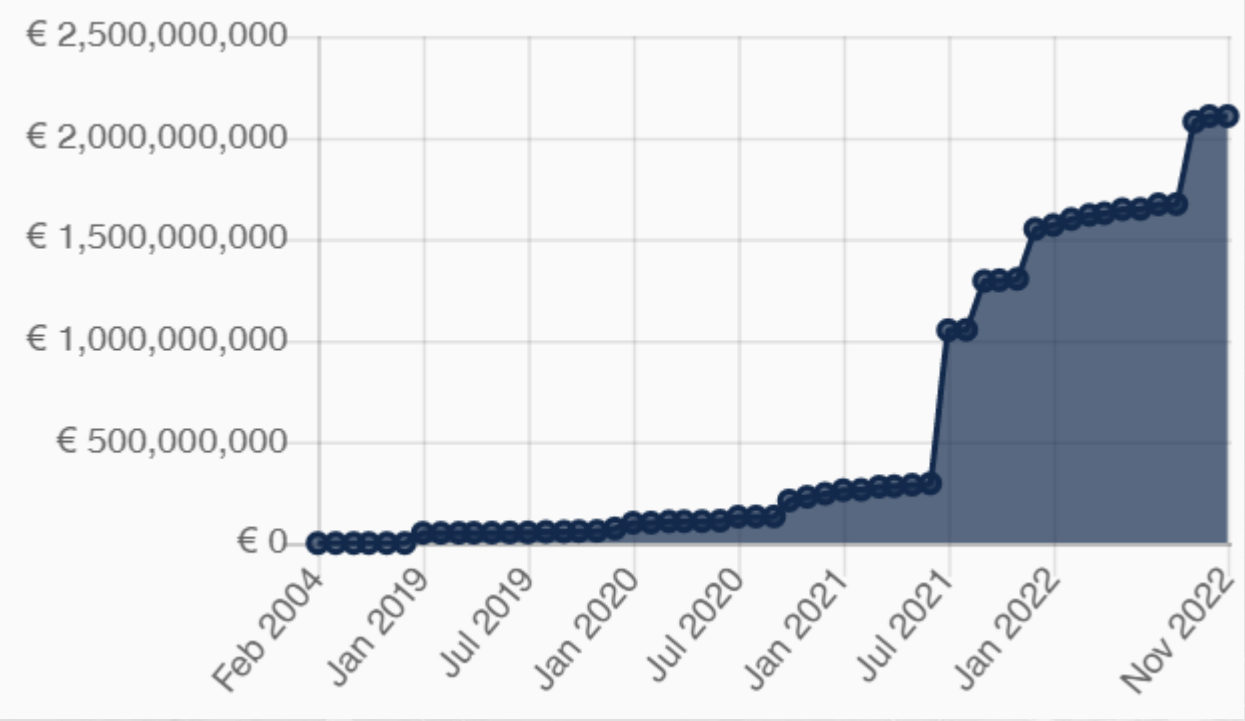
- GDPR
- ePrivacy

Phase 2 2010-2020

Create European digital single market

- Investment programme
- Legislative package
- Digital Sovereignty

Should enforcement be taken seriously?



Source: GDPR Enforcement Tracker - list of GDPR fines

Cumulative GDPR fines €2.1bn

1350 enforcement actions