Organisers

AAIL ASIAN ACADEMY OF INTERNATIONAL LAW

AAIL FOUNDATION

Privacy, Cybersecurity and AI

Mr Cédric Burton

Partner, Global Co-Chair of Privacy and Cybersecurity
Wilson Sonsini

WILSON SONSINI

Agenda

I) Recent trends in GDPR enforcement

I) Artificial Intelligence

1) How does GDPR apply to AI
2) Upcoming AI Act's impact on businesses

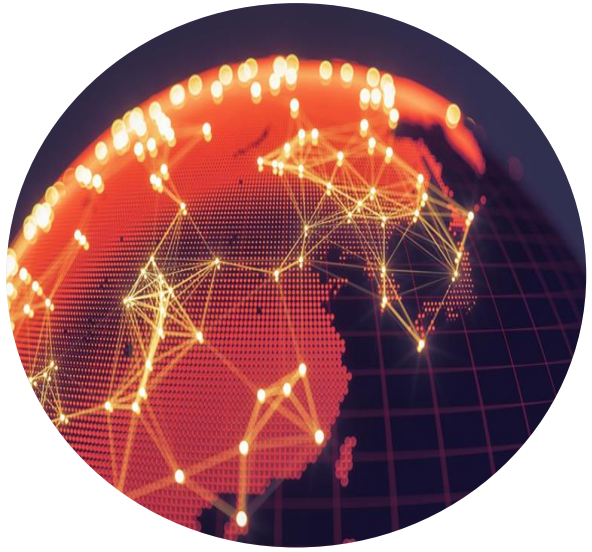
I) Overview of EU Digital Acts

1) Digital Services Act (DSA)
2) Digital Markets Act (DMA)
3) NIS2
4) DORA
5) Data Act

WILSON SONSINI

I. Recent Trends in DPR Enforcement

Transfers



Meta Facebook Service (IDPC – May 12, 2023)

- **Suspend EU-US transfers within 5 months**
- **+ pay € 1.2 billion fine** (largest GDPR fine ever)
- **+ order to bring processing into compliance with GDPR within 6 months.**

Decision concluded that:

  - Meta infringed GDPR Art. 46(1) by continuing to transfer personal data from the EU to the US while failing to guarantee individuals' 'essentially equivalent' protection

  - Standard Contractual Clauses (SCCs) relied upon by Meta provided inadequate safeguards and did not effectively address the risks to fundamental rights and freedoms of EU data subjects

  - Meta must cease unlawful processing, including storage, in the US of personal data of EU users transferred in violation of GDPR

- Following GDPR Art. 65 proceedings

- Meta has indicated it will appeal the decision and will apply to the High Court of Ireland to stay the orders
  - Creates more pressure on EU-US Data Privacy Framework to pass before Fall

Transparency and Legal Basis

WhatsApp (Irish DPC – September 3, 2021)

- **€ 225 million fine + order to remediate within 3 months**
- Violation of GDPR transparency requirements and overarching transparency principle
  - ***Content***: more detail than market practice (e.g. legal basis)
  - ***Format***: inconsistencies in linked documents + must cover all information
- Following GDPR Art. 65 proceedings



Meta IE (December 31, 2022) and WhatsApp (January 19, 2023) – Irish DPC

- **Facebook and Instagram (together Meta IE) fined €390 million (cumulatively) + order to remediate within 3 months**
- **WhatsApp fined €5.5 million + order to remediate within 6 months**
- Meta did not sufficiently explain the legal basis for processing personal data
- 'Performance of a contract' legal basis cannot be relied upon for:
  - Personalized ads to users (Meta IE)
  - Service improvement and security (WhatsApp)
- Following GDPR Art. 65 proceedings

Cookies

Facebook, Google, Microsoft, Amazon, TikTok, Roularta decisions (various DPAs)

- **Website operators using Google Analytics ordered to assess and implement supplementary measures** (e.g. pseudonymization by 'reverse proxy') or cease use
  ≠ 'ban on the use of Google Analytics'
- **CNIL fines**:
  - **Google € 150 million and Facebook € 60 million** for failing to provide an option to easily reject all cookies
  - **Google € 100 million** for (1) placing non-essential marketing cookies without prior user consent; (2) failing to provide users with information on such automatic placement of cookies, and (3) allowing an advertisement cookie to continue gathering information after personal ad deactivation.
  - **Amazon € 35 million** for automatically storing cookies on user devices without prior consent, when users were redirected to Amazon's French website by clicking on an Amazon ad on third-party websites.
  - **Microsoft € 60 million and TikTok € 5 million** for failing to make it as easy to reject cookies as it is to accept them on bing.com; and, in the case of TikTok, also for failing to inform users in a sufficiently precise manner of the purposes of the different cookies

- **Belgian DPA fined Roularta Media Group € 50,000** for failing to obtain consent for statistical cookies

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DATATILSYNET

CNIL.

dsb Republik Österreich Datenschutzbehörde

Children's Data

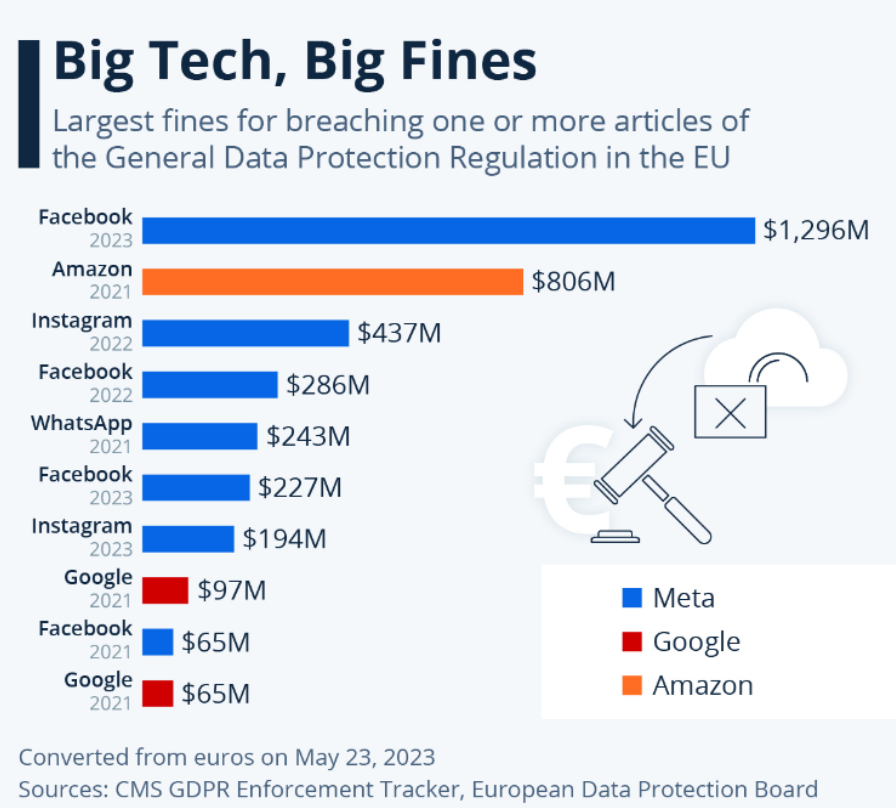
Instagram (IDPC – September 15, 2022)

- **Fined € 405 million**
- Public disclosure of contacts details
- Violation of legal basis, data minimization, transparency, PbD and DPIA
- Sets children's privacy at the top of the agenda

TikTok (ICO – April 4, 2023)

- **Fined £ 12.7 million (€ 14.6 million)**
  - Processed data of children under the age of 13 without appropriate parental consent
  - Privacy notice not sufficiently concise, transparent and easily understandable, and
  - Processing special category data without appropriate legal ground

The Enforcement Life Cycle



Source: Statista, https://www.statista.com/chart/25691/highest-fines-for-gdpr-breaches/

1
First DPA decisions with relatively low sanctions
DPAs issue decisions and companies are reluctant to sue as too expensive or cases are too difficult to defend

2
Higher DPA fines
DPAs impose higher fines and companies will start to challenge sanctions before national courts and the CJEU

3
Courts follow DPAs
National courts and the CJEU will broadly follow DPAs, except on procedural issues and general principles of law

4
Courts limit DPAs powers
National courts, and in particular the CJEU, will start limiting the powers of DPAs and overturning their decisions

Enforcement Priorities

AI	• National DPAs already enforcing against generative AI applications • EDPB has created a taskforce to coordinate national DPA activities
Cookies	• Apps and collection of data via SDKs are the next target • The CNIL is and will stay active • We expect the Google Analytics saga to continue (other countries to follow)
EDPB focus areas	• Coordinated enforcement action on the role and position of data protection officer launched in March 2023
Children's data	• Expect a number of significant decisions in the field
Other types of sensitive data	• Management of health files and mobile apps a CNIL enforcement priority
Joint Controllership trend	• Existing CJEU decisions (Jehovah witness, FashionID) • DPAs are increasingly finding that companies are (joint) controllers for specific activities • Visible in the ad tech context but more broadly in the C2C context

WILSON SONSINI

II. Artificial Intelligence

1) How does GDPR apply to AI

Key GDPR Principles

- Roles and responsibilities
- Purpose limitation
- Establish a legal basis
- Data minimization
- Transparency
- Automated Decision Making
- Data subject rights
- Data Retention

GDPR and AI: Key Considerations

Roles and Responsibilities

Parties may have different roles under the AI Act and the GDPR

AI Act:
- Providers
- Users
- End-users

GDPR:
- Controller
- Processor
- Data subject

Transparency

Information must be 'concise, understandable, and easily accessible'

- **Data collected directly from individuals** must be provided at the time of collection
- **Data collected from other sources** must be accompanied with a mechanism to provide the information within reasonable time

Legal Basis

Any use of personal data to develop, train and deploy AI systems requires a legal basis

GDPR provides for six legal bases:
- Consent
- Contract
- Legitimate interests
- Legal obligation
- Necessity
- Public interest

Data Subject Rights

Obtain **access** to data (e.g. confirmation of processing, receive a copy of the data)

Rectify outdated or wrong data

Request **deletion** of data ('right to be forgotten')

Data **portability** (e.g. transmit the data to another company)

Not to be subject to Automated Decision-Making

Object to processing (e.g. based on LI) or **restrict** processing

- **Broad interpretation of 'ADM' (see AG opinion in C-634/21, *Schufa I*)**
- **Individuals have the right to challenge ADM and request human intervention**

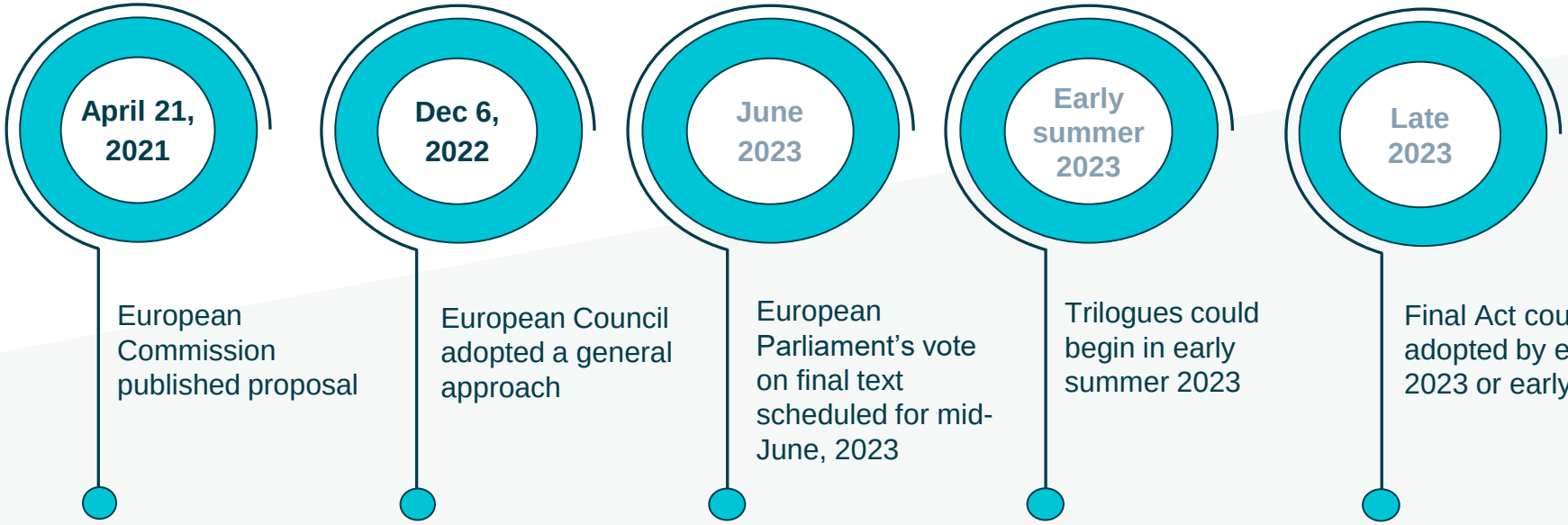
WILSON SONSINI

II. Artificial Intelligence

2) Upcoming AI Act's impact on businesses

The AI Act: Timeline

- **A new law to regulate AI systems**
- Current text of the AI Act will still change. EU Commission proposed a draft in 2021, which is now being discussed by the co-legislators: the EU Council and EU Parliament. The EU Parliament aims to agree on their proposed amendments in the coming days, to initiate talks between the three institutions still this summer



The AI Act: Current Scope

The AI Act is broad in scope

Any 'AI System' could trigger requirements:

- **Broad, technology-neutral definition of 'AI Systems'**, including 'machine learning', 'logic and knowledge based' systems and 'statistical' approaches
- Includes standalone AI systems and those integrated into products

Obligations could apply to:

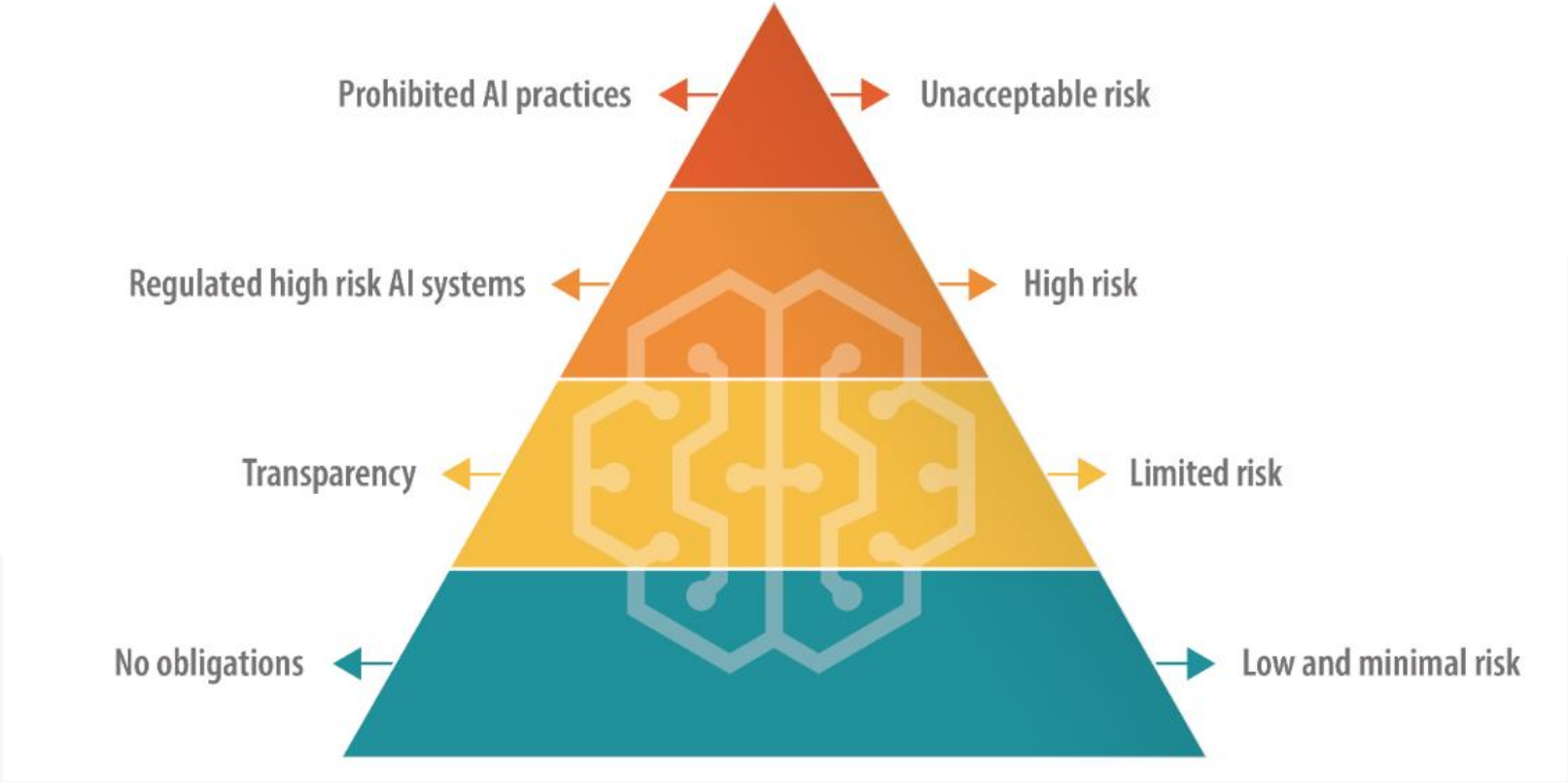
- **Providers** of AI systems on the EU market, regardless of where they are established
- **Users** of AI systems located in the EU
- **Providers or users of AI systems in a third country**, where the output produced by the systems is used in the EU

Similar to the GDPR, it is likely that many non-EU companies abroad will comply with the AI Act given the practicality of having a unified global approach.

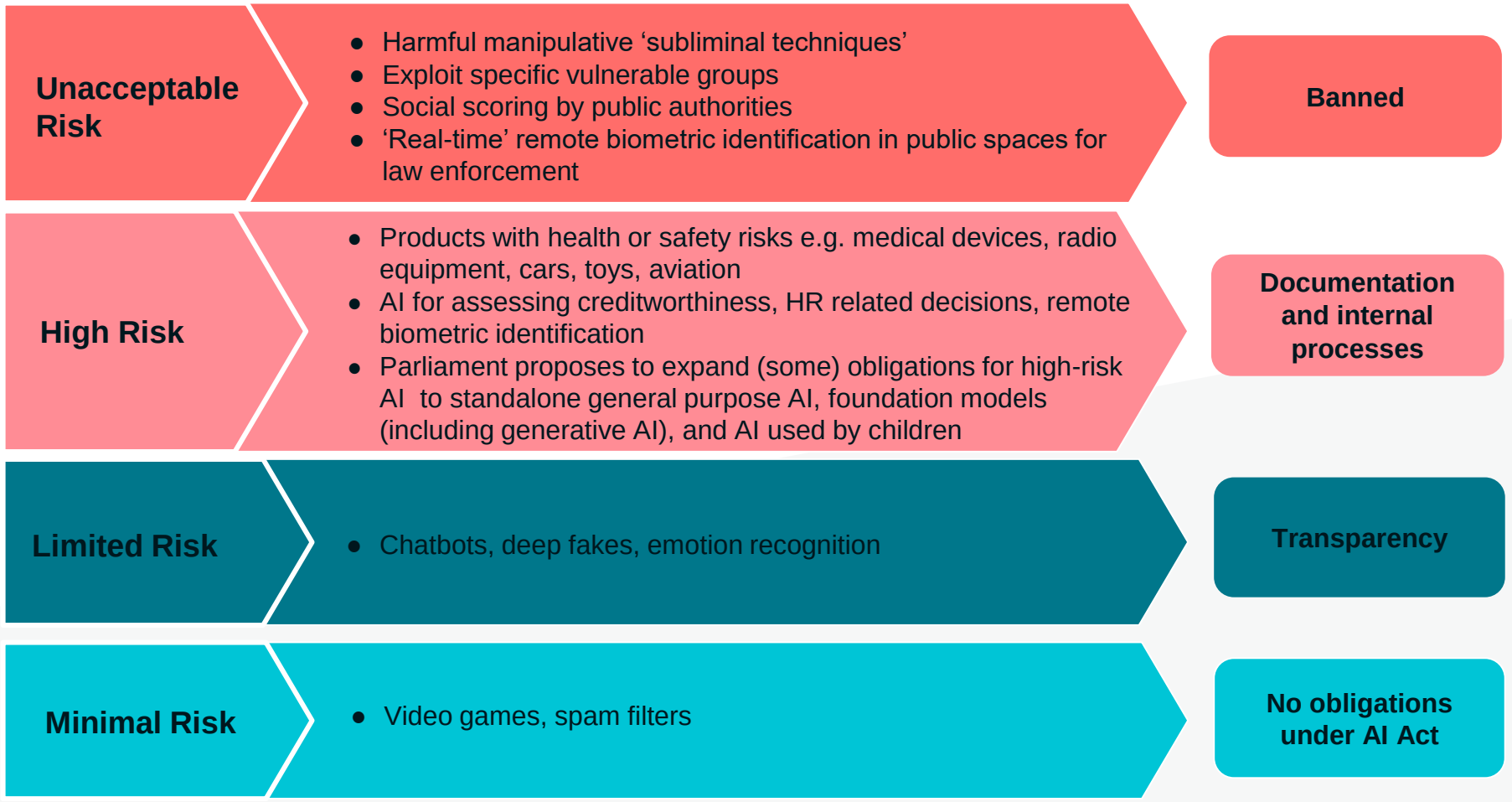
Potentially more direct obligations for vendors in third-countries than under the GDPR

The AI Act: Categorization of AI Systems

- The EU's proposal focuses on categorizing different types of AI and AI uses into different levels of risk categories with different rules and restrictions for each:



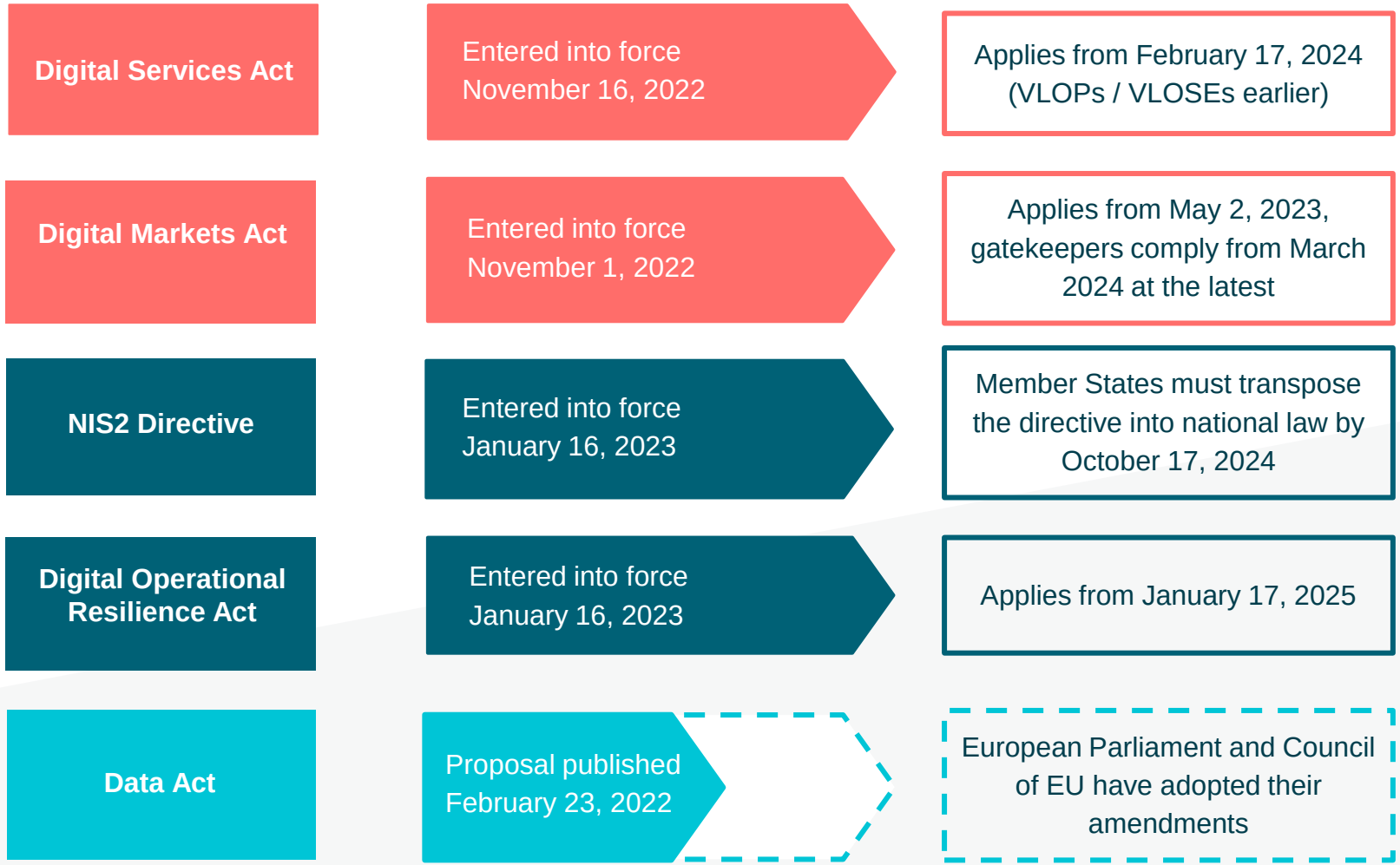
The AI Act: Risk Levels – Examples



WILSON SONSINI

III. Overview of EU Digital Acts

New Digital Acts Timelines



Digital Services Act: Scope

- The Digital Services Act (DSA) imposes new obligations on digital services companies operating in the EU

Mere conduit and caching services	Provide communication transmission networks e.g. internet access providers or domain name registrars
Hosting Services	Store information at the request of the customer e.g. cloud service provider or website hosting services
Online Platforms	A subcategory of hosting services that disseminate information to the public, including online marketplaces, app stores, social networks, etc.
Very Large Online Platforms or Search Engines	Online platforms or search engines that have more than 45 million users in the EU

Digital Services Act: Key Obligations

Obligations to remove illegal content

Increased transparency requirements, especially in relation to online advertising and content moderation

Prohibition of profiling sensitive, e.g. health, and children's personal data

- Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs) will be subject to more stringent obligations
- Fines for non-compliance are high, reaching a maximum of up to 6% of a company's annual worldwide turnover

Digital Markets Act

The DMA requirements will apply to designated ***gatekeepers***:

1) has an average market value of at least €75 billion, or an annual EU turnover of at least €7.5 billion in each of the past three years, and provides the same core platform service in at least three EU countries; and
2) has, on average, at least 45 million active monthly end-users in the EU and at least 10,000 yearly business users in the EU, in the previous three years.

First designations by the European Commission (EC) expected in September 2023

Restrictions on how gatekeepers can use data

New transparency requirements, especially in relation to advertising

Requirements to share data with users and third parties

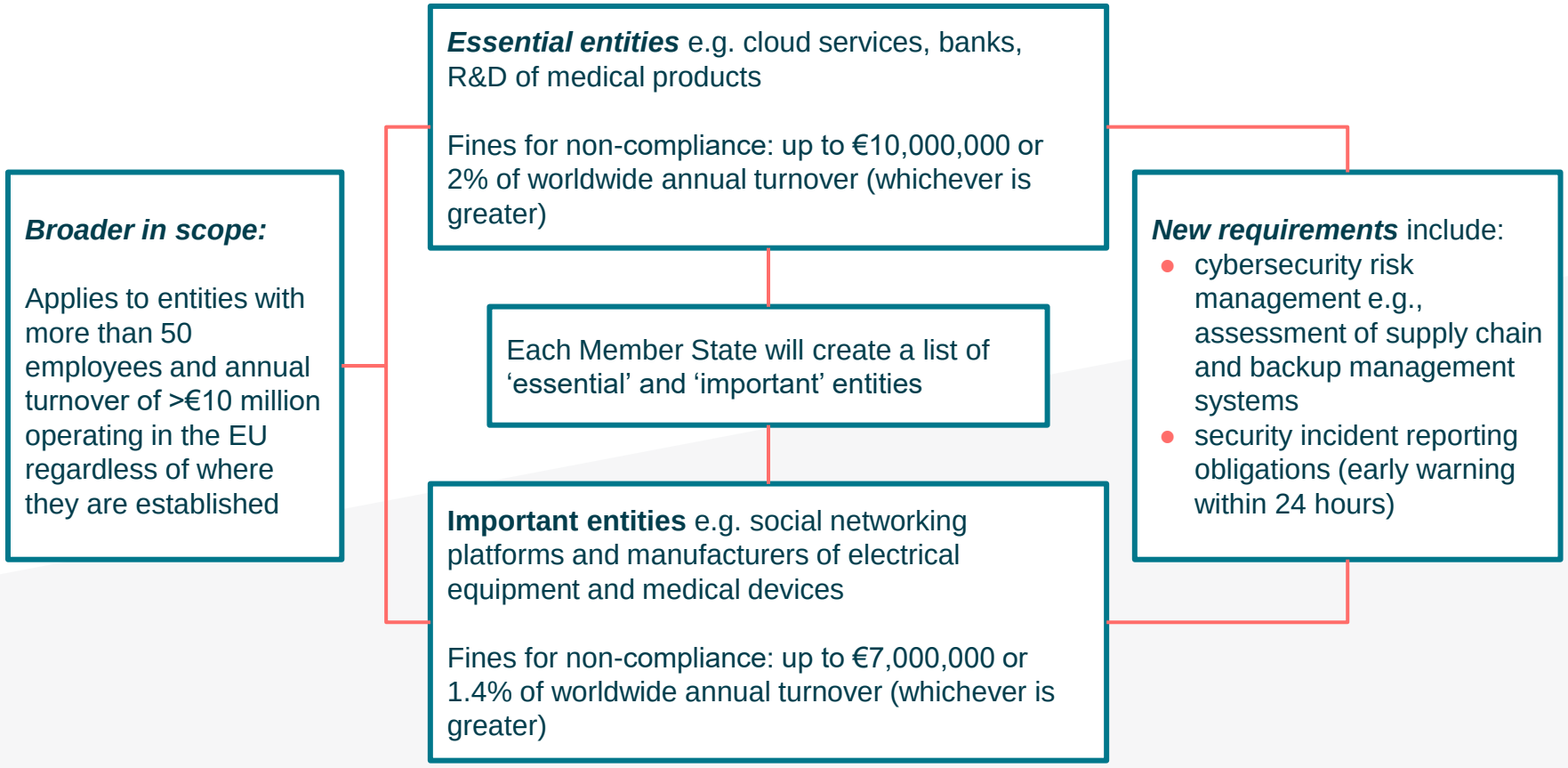
The DMA will be enforced by the EC:

(1) Fines up to 10% of annual worldwide turnover raising to up to 20% annual worldwide turnover for repeated infringements;

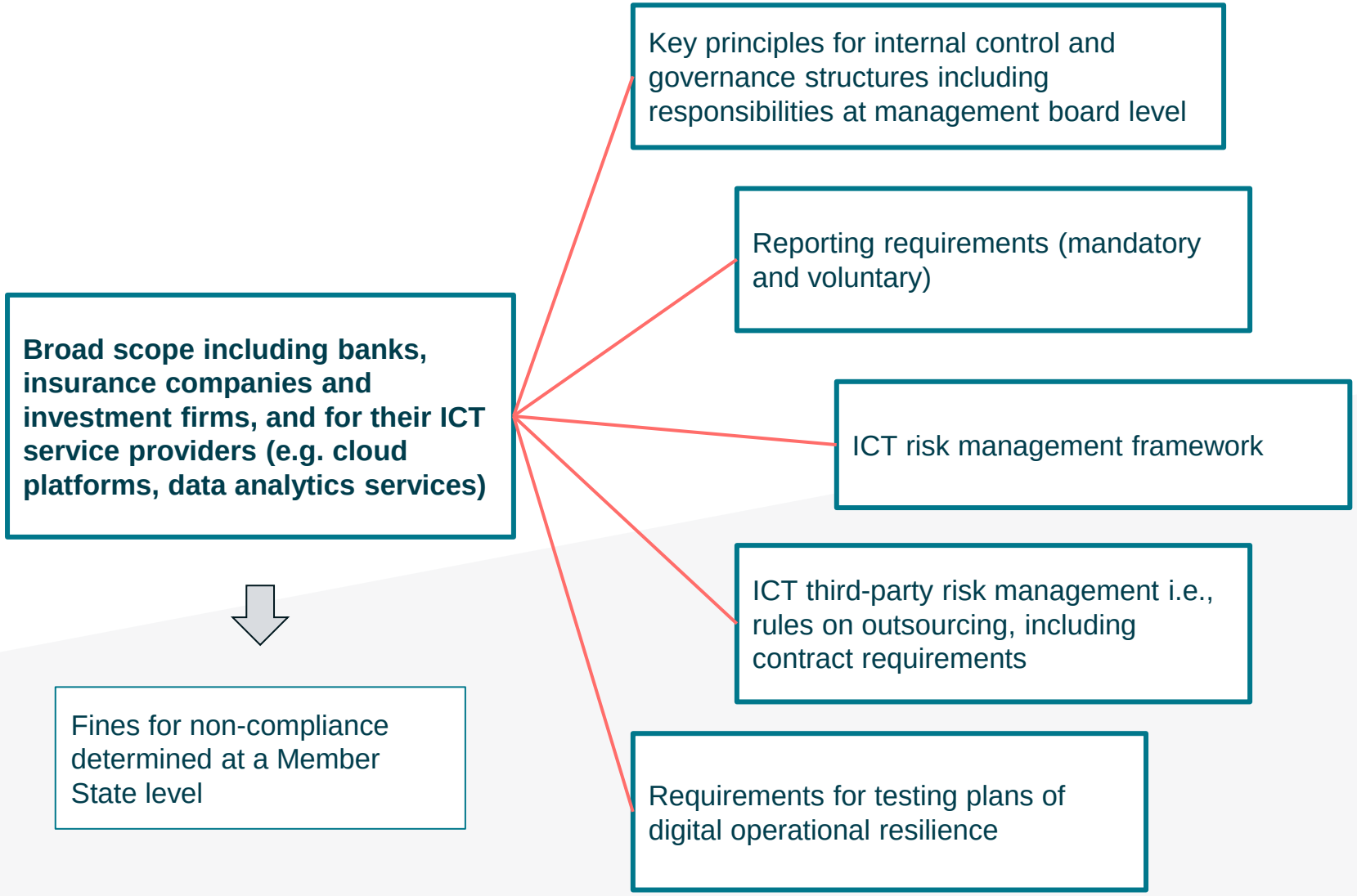
(2) In cases of continuous non-compliance (3 infringements in 8 years) the EC is empowered to conduct or order structural remedies e.g. breakup companies or forced divestments.

NIS 2 Directive

The new ***EU cybersecurity directive (NIS2)*** will replace the current security of network and information systems (NIS) directive.



Digital Operational Resilience Act



The Data Act

- The Data Act is a key pillar of the European Data Strategy and creates new rules on who can use and access data generated in the EU across all economic sectors

The **European Strategy for data** (2020) aims to make the EU a leader in a data-driven society

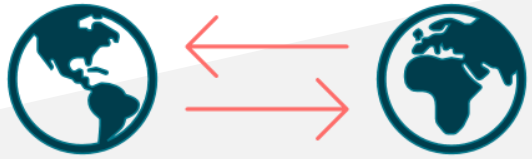
The **Data Governance Act** (2020) facilitates data sharing across sectors and Member States

The **Data Act** (2022) clarifies who can create value from data

Nine **European common data spaces** running from industry to mobility, from European Green Deal to energy and health

Data Act: Overview

- The Data Act will apply to personal and non-personal data and is without prejudice to the GDPR



Data sharing requirements apply to data generated by connected products and related services

Cloud service providers must comply with switching obligations

Restrictions on transfers of non-personal data outside the EEA

WILSON SONSINI

Thank you

Cédric Burton
Partner, Global Co-Chair of Privacy and Cybersecurity
Privacy and Cybersecurity
Brussels
cburton@wsgr.com