# Europe's Digital Rulebook: Privacy, AI, Enforcement, and the Global Impact

**Nik Theodorakis**
Wilson Sonsini

**Rohan Massey**
Ropes & Gray

Privacy+ Security Forum

# Speakers

## Nik Theodorakis

Partner
Wilson Sonsini

## Rohan Massey

Partner
Ropes & Gray
(London)

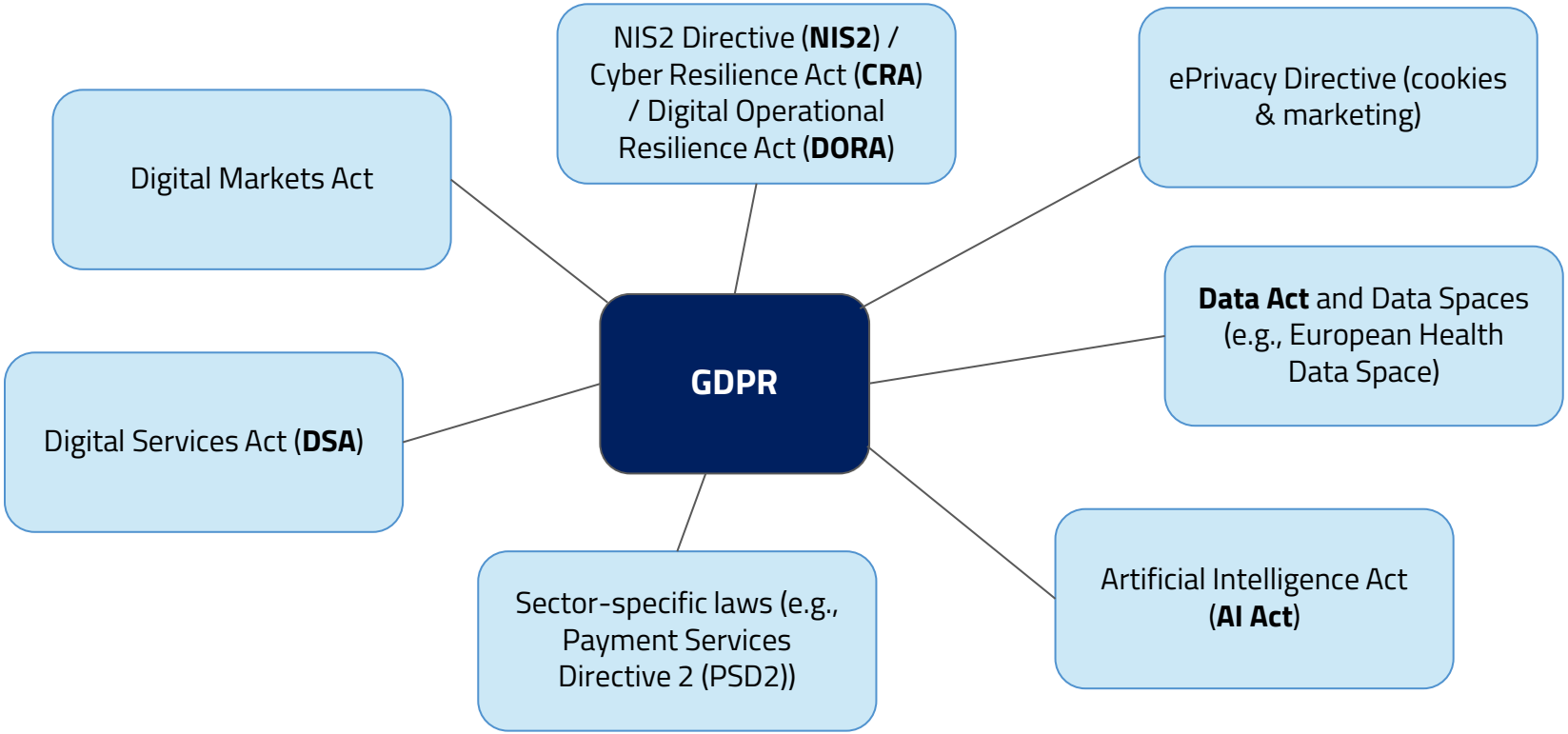
# Agenda

1. Introduction: The EU as the World's Digital Regulator
2. The Four Pillars of the EU Digital Rulebook
3. Global Reactions: How the UK and US Are Responding
4. The EU Digital Omnibus Proposal: A New Direction?
5. Enforcement: Balancing Regulation and Innovation
6. Geopolitical Currents: UK, US and EU Dynamics
7. Questions and Discussion

# Introduction: The EU as the World's Digital Regulator

Privacy+ Security Forum

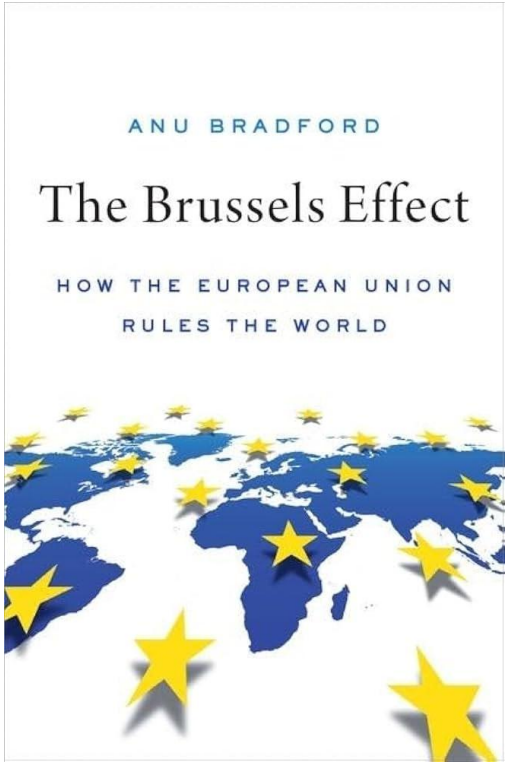
# EU Digital Regulatory Framework



# The Brussels Effect

Privacy+ Security Forum

- Brussels Effect is the idea that "*the EU has the unique ability among nations today to promulgate regulations that shape the global business environment, elevating standards worldwide and leading to a notable Europeanization of many important aspects of global commerce*"
- Major area of EU soft power as EU rules can become a de facto global standard
- Impact in practice:
  1) From the company's perspective, EU market size and stringent standards make it economically practical to comply with EU standards even outside the EU market
  2) From a state perspective, the EU's proactive stance provides inspiration for new regulation
- GDPR is a strong example, but other digital regulations are yet to have the same effect



# The Four Pillars of the EU Digital Rulebook

Privacy+ Security Forum

# The Four Pillars of the EU Digital Rulebook

Privacy+ Security Forum

| | Regulation or Directive | Subject Matter |
|---|---|---|
| 01 | **GDPR** | Regulates processing of personal data |
| 02 | **DSA** | Creates a framework for regulating digital services and protecting consumers online |
| 03 | **Data Act** | Aims to facilitate data access, use and sharing across the EU and encourage competition in the cloud market |
| 04 | **AI Act** | Sets horizontal, risk-based rules to regulate the development and use of AI systems and models |

# GDPR - 8 years on

Privacy+ Security Forum

- **Compliance approaches are maturing** as basic privacy requirements become widely adopted and companies develop more sophisticated legal positions across jurisdictions
- **Enforcement is evolving but friction remains.** DPAs adopt strategic priorities, and cooperation is improving. Challenges remain as authorities seek to assert jurisdictional competence. The GDPR Procedural Regulation will apply to new investigations started after April 2027
- **New technologies are challenging GDPR principles** (e.g., agentic AI compliance with GDPR principles, or exercising right to be forgotten for blockchain technologies)
- **Increasingly significant overlap between privacy and other areas of digital regulation** (e.g., design and operation of online services may face regulation under the DSA, GDPR, and consumer protection laws)

# DSA: Key points to know

Privacy+ Security Forum

| | | | |
|---|---|---|---|
| 1 | Applies to “intermediary services” including online platforms and online marketplaces | 5 | Sets due diligence requirements for online marketplaces |
| 2 | Obligations tiered according to size and nature of the service | 6 | Prohibits dark patterns and deceptive design |
| 3 | Introduces requirements to take action on illegal content | 7 | New advertising requirements, including restrictions on using certain data for advertising |
| 4 | Enhances transparency obligations, including of recommender systems | 8 | Includes a broad requirement to ensure minors are safe online |

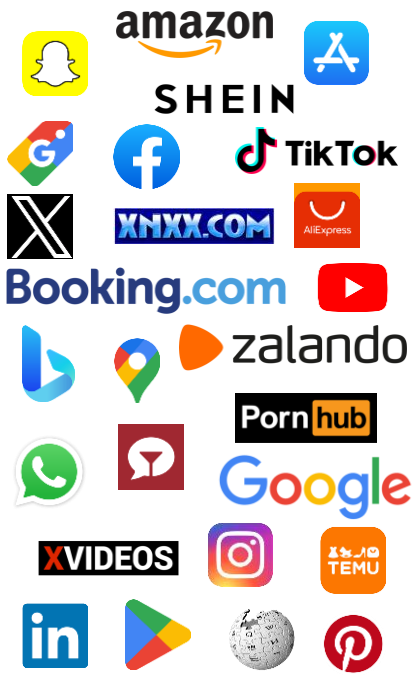
# DSA: Enforcement (European Commission)

Privacy+ Security Forum

**The European Commission (EC) is responsible for enforcing the DSA for Very Large Online Platforms (VLOPs) / Very Large Online Search Engines (VLOSE):**

- On December 5, 2025, the EC issued its first penalty under the DSA. It fined X €120 million because:
  - X's use of the "blue checkmark" was deceptive
  - X's ad repository lacked transparency
  - X failed to provide researchers access to public data
- The EC has multiple ongoing investigations. It has issued preliminary findings but no further fines
- Examples of the EC's key focus areas include:
  - Failing to protect minors online and assessing risks for minors
  - Use of deceptive and addictive design
  - Transparency obligations, including of recommender systems
  - Presence of illegal content or products
  - Risk assessments and mitigations

Designated VLOPs/VLOSEs:



# Data Act: Key points to know

Privacy+ Security Forum

| | | | |
|---|---|---|---|
| 1 | Broad, extra-territorial scope | 5 | Restricts sharing of non-personal information data (stored in the EU) with non-EU authorities |
| 2 | Forms the backbone of the EU single market for data, together with the Data Governance Act | 6 | Limits the enforceability of “unfair” data terms in B2B agreements |
| 3 | Allows EU customers of SaaS, IaaS, and PaaS providers to switch to another provider | 7 | Requires sharing data with EU authorities in emergencies |
| 4 | Allows IoT users to access data generated by connected hard/software | 8 | Enforced at national level with penalties of up to 10% worldwide annual turnover |

# Data Act: Practical considerations

Privacy+ Security Forum

## Current state of play…

In principle, the Data Act is very broad and impactful but so far the market is adopting a "wait and see" approach:

- The framework to enforce the Data Act is not yet in place in many (17) EU countries
- The European Commission is developing guidance on definitions of key Data Act concepts and model contractual clauses
- Amendments have been proposed under the Digital Omnibus (e.g., on switching requirements) creating some legal uncertainty

## Steps companies can take today…

- Consider amending template contracts (e.g., manufacturers of IoT devices could add a Data Act addendum governing the terms of data access (to the extent permitted by law))
- Review how switching can be technically achieved
- Map relevant data flows that could be affected by access/ switching provisions
- Monitor market practices and national variations (e.g., France banned switching charges a year before the Data Act deadline (since Dec. 1, 2025))

# AI Act: Key points to know

Privacy+ Security Forum

| | | | |
|---|---|---|---|
| 1 | Broad, extra-territorial scope | 5 | Bans certain applications of AI |
| 2 | Does not apply to areas outside of EU Law (e.g., national security or military uses) | 6 | Majority of obligations focused on high-risk applications of AI |
| 3 | Applies to actors throughout the AI supply chain | 7 | Transparency obligations for AI that poses specific risks |
| 4 | Horizontal/ Cross-sector approach | 8 | Separate obligations for providers of general purpose AI |

# AI Act: Framework still developing

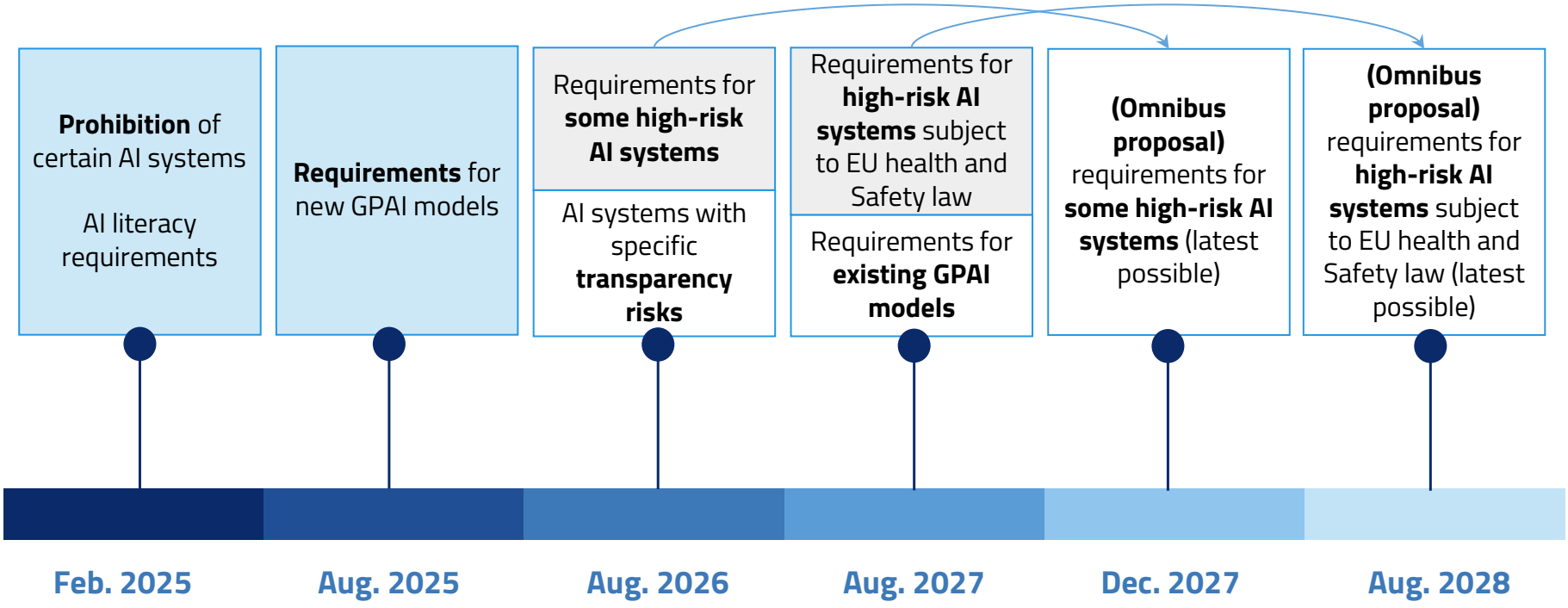
Privacy+ Security Forum

- **Phased implementation in progress.** Obligations are becoming applicable in stages (from Feb. 2025), but most high-impact requirements are still to come
- **Industry grappling with first-of-its-kind complexity.** Applying the AI Act requirements against a backdrop of accelerating innovation is practically and technically challenging
- **Bottleneck of soft law.** Codes of practice and guidance are critical for implementation but work is delayed. The code of practice on general purpose AI was published in July 2025, 3 weeks before the compliance deadline
- **Overlap in a complex regulatory framework.** The interaction between the AI Act and other EU laws (e.g., GDPR, sector-specific laws and cybersecurity laws) lacks clarity. Guidance on the relationship between the GDPR and the AI Act is expected
- **Fragmented enforcement structure still developing.** The AI Act relies on a complex, multi-layered enforcement system (EU, national and sector regulators). For example, 15 regulators have been appointed in Ireland. Most countries are delayed in operationalizing the enforcement system
- **National nuances emerging.** Some countries are adding requirements in national law (e.g., Italy's AI Act implementing law includes additional protections for under-14s)

# AI Act: Implementation timeline

Privacy+ Security Forum

Against the backdrop of regulatory uncertainty, institutional bottlenecks and industry pushback, the timeline for application may change:



# Global Reactions: How the UK and US Are Responding

Privacy+ Security Forum

# The United Kingdom's Post-Brexit Path

Privacy+ Security Forum

Since exiting the EU in 2020, the UK has taken its own regulatory agenda:

**Aligned** ← → **Diverged**

**Privacy** - balancing regulatory divergence while maintaining adequacy

- The Data (Use and Access) Act amended but did not overhaul the retained GDPR
- The EU formally recognized that amended UK data protection law offers an essentially equivalent level of protection as the GDPR

**Cybersecurity** - flexible and targeted approach to specific threats

- Draft bill proposes to amend existing UK cybersecurity law (retained EU law) to broadly align with NIS2 (does not go as far)
- Scaled back equivalent to the CRA exists
- No equivalent to DORA

**Artificial Intelligence** - principles-based, pro-innovation approach

- No statute regulating AI
- ICO preparing legally binding code of practice
- Principles-based approach relying on regulatory coordination and sectoral enforcement

**Online Safety** - statutory framework focused on harms

- The Online Safety Act 2023 focuses on online harms and safety duties
- Limited overlap with the DSA

# UK: Amending privacy laws in practice

Privacy+ Security Forum

| Topic | EU Baseline | UK Amendment | Practical Impact of UK Amendment |
|---|---|---|---|
| **Cookies** | Consent required for non-essential cookies | **Consent not required for limited low-risk uses** (e.g., statistical purposes, adapting service appearance/functionality to user preferences). Higher potential penalties | Narrow but meaningful relaxation for low-risk analytics and UX optimization |
| **Providers of services accessible by children ("Providers")** | No specific cross-cutting obligation for Providers | Providers must implement **age-appropriate child-protection safeguards, accounting for age groups and developmental stages** | Providers need to evidence steps taken to comply (aligns with UK Age Appropriate Design Code in practice) |
| **Automated decision-making ("ADM")** | Strict limits on ADM with legal/similar effects. Typically requires consent or narrow exceptions | **Permits ADM** using non-sensitive data if **safeguards are in place**, including (e.g., right to contest and human review) | Easier to use ADM technologies when special category data is not processed |

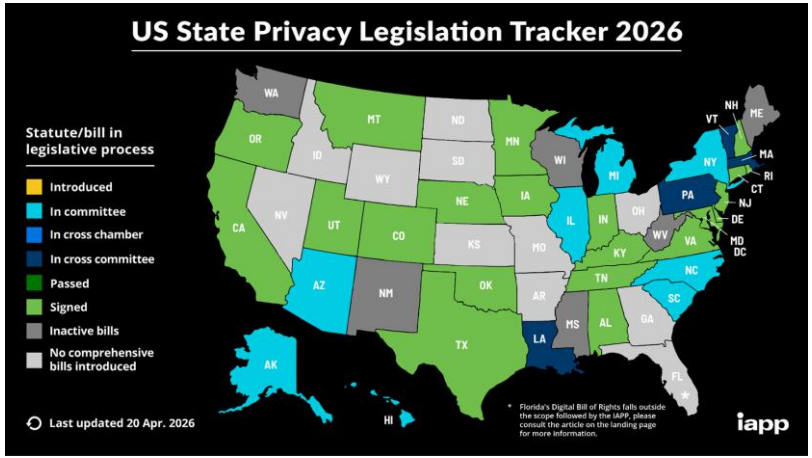
# UK: Amending privacy laws in practice

Privacy+ Security Forum

| Topic | EU Baseline | UK Amendment | Practical Impact of UK Amendment |
|---|---|---|---|
| **Scientific/ statistical research** | Reuse permitted for "scientific/statistical research" (scope undefined in law). New non-binding guidance offers some flexibility for commercial purposes | Clarifies that **scientific research includes commercial and privately funded activity** (e.g., product development and testing) | Expands ability to reuse data for R&D and AI development with legal certainty |
| **Legitimate interest as a legal basis for processing** | Available subject to case-by-case balancing test. Examples provided in non-binding guidance only | Introduces a **statutory list of recognized legitimate interests** (e.g., crime prevention) | Greater legal certainty in defined scenarios; reduces reliance on balancing test |
| **Data subject access requests ("DSARs")** | 1-month response deadline with broad search expectations | Allows controllers to: **pause the deadline** to seek clarification, limit responses to a **"reasonable search"**, request more detail where processing is extensive | Additional reassurance when resisting over-broad or complex DSARs |

# The United States' Evolving Position

- **Fragmented regulatory framework.** Privacy is governed at state level, no federal privacy law. Formed of general (e.g., CCPA) and sector-specific data privacy regulations (e.g., COPPA and HIPAA)
- **Broader focus on consumer protection than EU privacy laws** (eg., targeting deceptive hidden fees, fake reviews)
- **Clash on content-moderation.** FTC prioritizes content moderation issues but from a different angle to Europe
- **No certain approach to AI.** No federal AI regulation but state laws are beginning to emerge (e.g., Colorado and Texas)
- **Strong pushback against extraterritorial EU laws** from American companies



# Regulatory Competition or Convergence?

Privacy+ Security Forum

Comprehensive, rights-based framework

Driven by fundamental rights (privacy, fairness, competition)

Ex ante, prescriptive rules

Aims to be a regulatory exporter ("Brussels Effect")

Sectoral, market-driven, fragmented

Focused on innovation, free markets, free-speech protections

Ex post enforcement, case-by-case

Pushing back on extraterritorial laws

Hybrid: principles-based with targeted intervention

Aims to balance innovation with accountability

Ex ante in specific areas (e.g., online safety), ex post in others (e.g., AI)

Positioning as bridge between EU and US

# The EU Digital Omnibus Proposal: A New Direction?

Privacy+ Security Forum

# What are the Omnibus Proposals?

- In November 2025, the European Commission published legislative proposals that aim to simplify the legal framework for data processing and AI to encourage innovation
- Formed of two parts (together, "Omnibus Proposals"):

**Digital Omnibus**

- Includes amendments to the GDPR, Data Act, e-Privacy rules, NIS2
- No timeline for the amendments to be passed
- Subject to intense negotiations

**AI Omnibus**

- Includes amendments to the AI Act
- Expected to be passed by summer 2026

- If enacted, the Omnibus Proposals would make important changes to the EU digital regulations framework

# Omnibus Proposal: Key draft changes

Privacy+ Security Forum

| Omnibus Proposal | Examples of Practical Implications |
|---|---|
| **Amend the GDPR definition of "personal data"**<br>→ Information will not be considered personal data for a given entity, if that entity has no reasonable way to identify the individual concerned | • Greater scope to argue that personal data does not qualify as personal data (not subject to GDPR) |
| **Consolidate cookie and tracking rules under the GDPR** and expand consent exemptions (e.g., by allowing aggregated audience measurement) | • One-stop-shop principles and GDPR-level penalties would apply to non-compliance with cookie rules |
| **Adjust data notification thresholds and processes**<br>→ Raise notification threshold for breaches that pose a "high risk" to individuals<br>→ Extend notification from 72 to 96 hours<br>→ Single EU-wide template<br>→ Single-entry reporting point (valid under GDPR, NIS2 and DORA) | • Fewer incidents would reach the threshold to report to regulators<br>• Report incidents under multiple laws via a single-entry reporting platform |

# Omnibus Proposal: Key draft changes

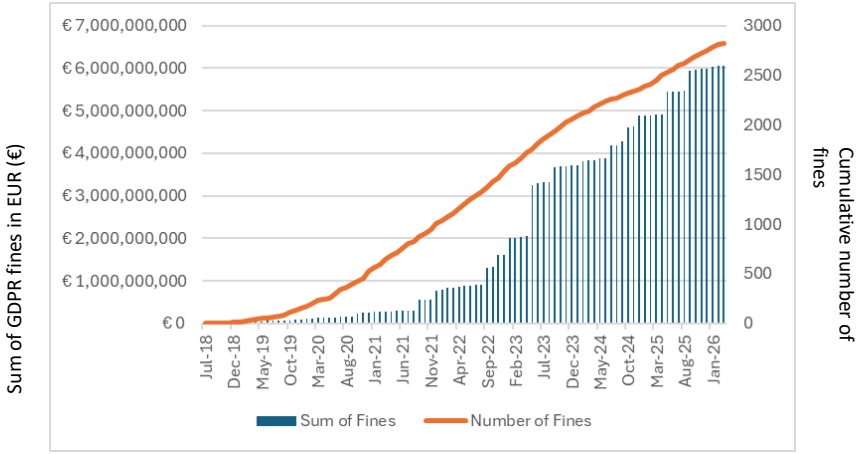
Privacy+ Security Forum

| Omnibus Proposal | Examples of Practical Implications |
|---|---|
| **"Legitimate interest" is a valid legal ground to develop and operate AI** provided certain conditions are met (e.g., conduct a "balancing test" and allow individuals to opt-out) | • Legal certainty: providers and deployers of AI do not need to obtain GDPR consent to train and operate AI |
| **Create new legal basis to process sensitive data for AI model training** provided attempts are made to identify and remove such data from the training dataset or use methods to prevent disclosure of the sensitive data in the output | • Easier to process sensitive data for AI model training |
| **Delay applicability of AI Act rules for certain high-risk AI systems** for 18 months | • Providers of high-risk AI systems (e.g., AI for assessing creditworthiness) would have longer to comply with the AI Act requirements |

# Enforcement: Balancing Regulation and Innovation

Privacy+ Security Forum

# Regulatory Trends: Current statistics




Source: https://www.enforcementtracker.com/?insights

## Top three countries to issue fines

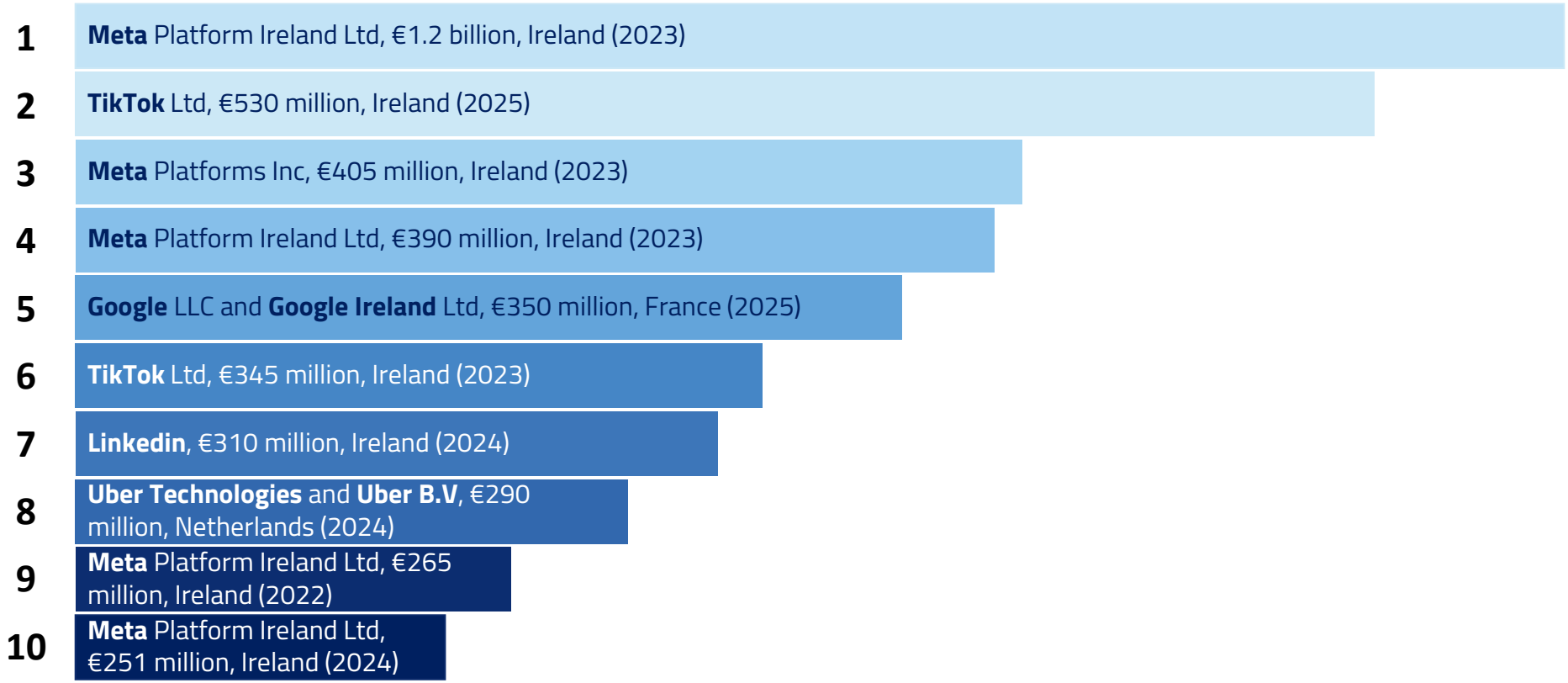
| By Value (EUR) | By Number |
|---|---|
| Ireland (4.03 billion) | Spain (1060) |
| France (888 million) | Italy (507) |
| Netherlands (372 million) | Romania (280) |

## Top three reasons for issuing a fine

- Insufficient legal basis for data processing
- Non-compliance with general data processing principles
- Insufficient security measures

# Enforcement Actions: Largest GDPR fines

Privacy+ Security Forum



# Top Priorities for European Regulators

Privacy+ Security Forum

## 2026 Priorities

CNIL.

1. Recruitment
2. Electoral registry
3. Sports federations

## 2026-2028 priorities

AUTORITEIT PERSOONSGEGEVENS

1. Mass surveillance
2. **Artificial intelligence**
3. Digital resilience

## EDPB 2026 Coordinated Enforcement Framework

edpb

European Data Protection Board

Transparency

## 2022-2027 Strategy

An Coimisiún um Chosaint Sonraí
Data Protection Commission

1. Regulate consistently and effectively
2. Safeguard individuals and promote data protection awareness
3. Prioritize the protection of children and other vulnerable individuals
4. Bring clarity to stakeholders
5. Support organizations and drive compliance

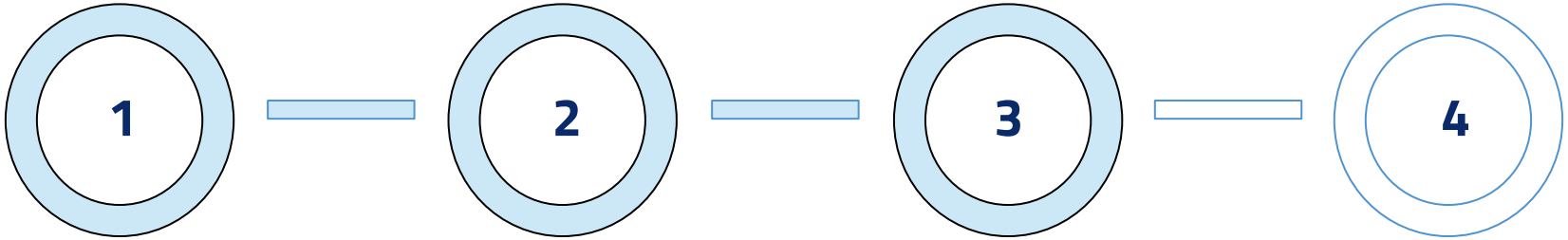
## 2025-6 Priorities

ico.

Information Commissioner's Office

1. **Automated decision-making**, including in government and in recruitment
2. **AI training**
3. Use of facial recognition by the police
4. **Emerging AI risks, including agentic AI**

# Enforcement Life Cycle




### First DPA decisions with relatively low sanctions

DPAs issue decisions and companies are reluctant to sue as too expensive and not worth it, or the cases are too difficult to defend

### Higher DPA fines

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

### Courts follow DPAs

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

### Courts limit DPA powers

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

# Geopolitical Currents: UK, US, and EU Dynamics

Privacy+ Security Forum

# Trade, Technology, and Regulatory Sovereignty

Privacy+ Security Forum

**EU's AI Act takes effect, sparking new Europe-US clash**

Key parts of the legislation governing artificial intelligence came into force on Saturday. Washington and American tech giants have not given up on their coordinated offensive against this law and, more broadly, against European digital regulation.

**EU fines on US companies are biggest source of friction, State Department official says**

**European Commission accused of 'massive rollback' of digital protections**

Proposed changes to AI Act would make it easier for tech firms to use personal data to train models without consent

**EU could water down AI Act amid pressure from Trump and big tech**

**U.S. raises concerns over EU tech rules as transatlantic tensions persist**

# Transatlantic Tensions and Data Flows

Privacy+ Security Forum

| Current Legal Position | Challenges | Results |
| --- | --- | --- |
| **EU–US data transfers require safeguards by default**, typically Standard Contractual Clauses (SCCs)<br><br>**Since January 2023, self-certified US companies under the EU-US Data Privacy Framework (DPF)** can receive EU personal data without additional transfer safeguards | • **Active and likely future challenges before the EU's highest court** after this court struck down the DPF's two predecessors<br>• **Political uncertainty in the EU** over durability of the DPF in the current geopolitical era<br>• **Insecurity caused by the potential that the key Executive Order** underpinning the DPF could be unilaterally amended/revoked by the US President<br>• **Oversight instability in 2025** after an oversight mechanism (PCLOB) lost quorum due to dismissal of three members by the Administration, raising concerns about continuity and independence of DPF supervision (later partially restored by court order) | Transatlantic tensions over data flows and legal uncertainty |

# Future-Proofing During Turbulent Times

Privacy+ Security Forum

1. Prepare for fragmentation in data flows and transfers (e.g., implementing SCCs as a "belt and braces" approach)
2. Documenting decisions and demonstrating proactive approach in the event of questions from regulators
3. Approach regulatory compliance strategically, focusing on key priorities and sectors
4. Focus on cybersecurity and resilience as the threat landscape evolves and will remain a priority during geopolitical turbulence
5. Broad, principles-based governance rather than detailed compliance checklist for each law can help reduce risks

# Questions & Discussion

Privacy+ Security Forum

# Thank you!

Privacy+ Security Forum