

May 8, 2024

EU Privacy + Security Law Workshop

Nik Theodorakis
Wilson Sonsini

Raphaël Dana
Dana Associés
(France)

Sarah Pearce
Hunton Andrews Kurth

Speakers



**Nik
Theodorakis**

Partner
Wilson Sonsini



Sarah Pearce

Partner
Hunton Andrews Kurth

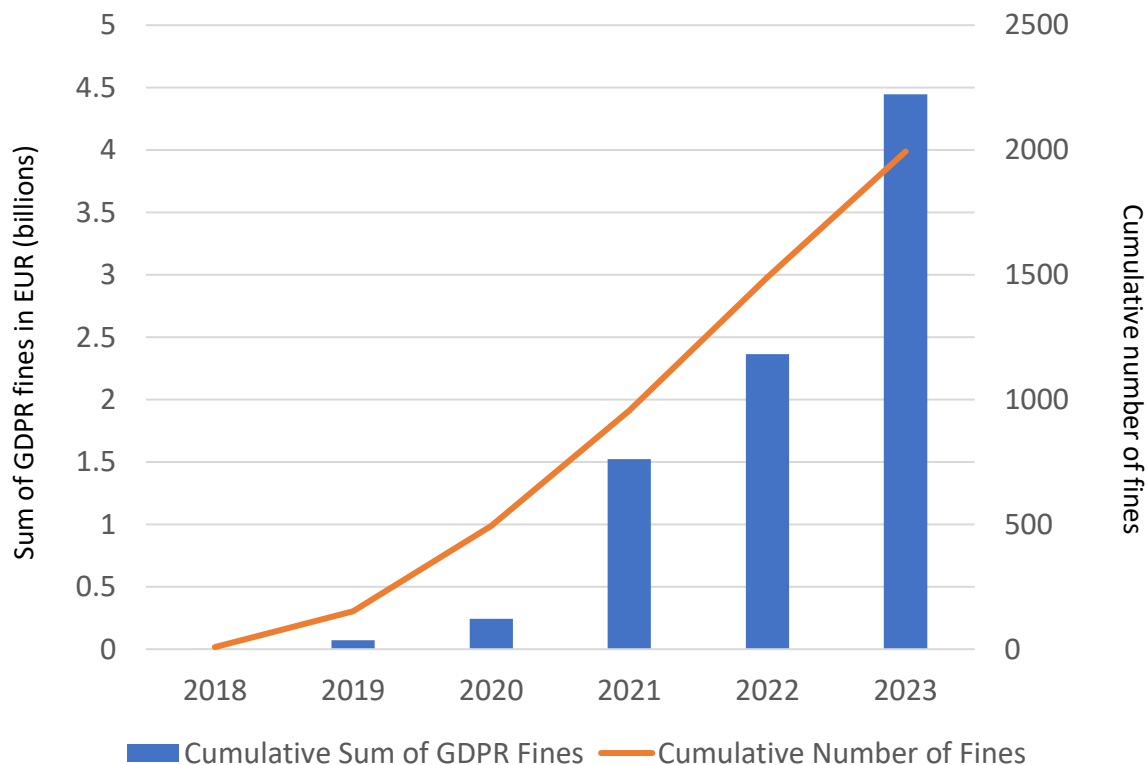


Raphaël Dana

Partner
Dana Associés
(France)







Regulatory Enforcement Trends

Regulatory Trends: Current Statistics



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

Top three countries to issue fines

By Value (EUR)		By Number	
	Ireland (2.8 billion)		Spain (825)
	Luxembourg (746 million)		Italy (353)
	France (371 million)		Germany (176)

Top three reasons for issuing a fine

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

Enforcement Actions – Largest GDPR Fines

1 **Meta** Platform Ireland Ltd, €1.2 billion, Ireland (2023)

2 **Amazon** Europe, €746 million, Luxembourg (2023)

3 **Meta** Platforms Inc, €405 million, Ireland (2023)

4 **Meta** Platform Ireland Ltd, €390 million, Ireland (2023)

5 **TikTok** Ltd, €345 million, Ireland (2023)

6 **Meta** Platform Ireland Ltd, €265 million, Ireland (2023)

7 **WhatsApp** Ireland Ltd, €225 million, Ireland (2023)

8 **Google** LLC, €90 million, France (2023)

9 **Facebook** Ireland, €60 million,
France (2023)

10 **Google** Ireland Ltd, €60 million,
France (2023)

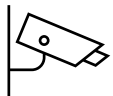
Recent Major CJEU Case Law



In September 2023, the IDPC fined Meta Platforms Ireland Ltd € 1.2 billion and issued an order to remediate within 6 months



Failure to sufficiently protect personal data for international transfers. The IDPC issued an order requiring Meta to suspend any future transfer of personal data to the US and an order to bring processing operations into compliance with the data transfers rules.



In January 2024, the CNIL fined Amazon France Logistique € 32 million



Failure to comply with the obligation to provide information and transparency on the video surveillance systems monitoring employees in warehouses.



In July 2023, the CNIL fined Criteo €40 million



Lack of consent in online advertising. Failing to verify that individuals had provided consent for their personal data to be processed.



In September 2023, the IDPC fined TikTok € 345 million



Non-compliance with GDPR rules regarding the processing of children's data including lack of transparency to children and not implementing privacy by design.



In January 2024, the CNIL fined Yahoo! € 10 million



Failing to respect the choice of users who refused cookies on the website and for not allowing the users of Yahoo mail to freely withdraw their consent to cookies.

Major CJEU Decisions in 2023 - 2024

Austrian Post, May 4, 2023

- Mere violation of GDPR does not give rise to the right to compensation.
- There must be a causal link between the infringement of the GDPR and material or non-material damage suffered.
- There is no threshold for seriousness of non-material damages.
- The GDPR does not prescribe rules for assessing damages.

Schufa II, Dec. 7, 2023

- Preparing credit scores can qualify as an automated decision making under Art. 22 GDPR.
- It did not matter that the ultimate decision, with legal or similar effect, was not taken by the entity that made the credit score.
- The credit score played a 'determining role' in the decision about whether to grant credit.

IAB Europe, March 7, 2024

- Character strings used to express users' preferences qualifies as personal data even though IAB did not hold the information to be able to identify the individual. IAB had reasonable means to obtain the identifier.
- IAB is a joint controller for the processing of users' preferences with websites, application providers, data brokers, and advertising platforms.

Top Priorities for European Regulators

2024 Priorities

1. AI
2. Cookies
3. Biometrics
4. Children's privacy



2024 Action Plan

1. Algorithms and AI
2. Big Tech
3. Freedom & Security
4. Data Trading
5. Digital Government



**EDPB Coordinated
Enforcement Framework**
Right of access



2022-2027 Strategy

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



2024 Priorities

1. **Children's data** use by online services
2. **Data subjects' access rights**
3. **Loyalty programs** and digital receipts
4. Data collected for 2024 Olympic and Paralympic Games



EDPB Work Program 2024-2027

Four key pillars of the EDPB work program



Enhancing Harmonization and Promoting Compliance

1. Produce guidance on key issues.
2. Support effective safeguards e.g., codes of conduct.
3. Develop information streams to complement guidance e.g., tailored to non-experts and SMEs



Reinforcing a Common Enforcement Culture and Effective Cooperation

1. Enforcement coordination e.g., Coordinated Enforcement Framework.
2. Effective functioning of One Stop Shop, issuing Opinions or Binding Decisions.
3. Support adoption of GDPR Procedure Regulation.



Safeguarding Data Protection in Developing Digital and Cross-Regulatory Landscape

1. Guidance on interplay between GDPR and other EU acts e.g., AI Act.
2. Promote human-centric approach to technologies.
3. Cooperate with other regulators on matters that impact on data protection.



Contributing to Global Dialogue on Data Protection

1. Support exchange and cooperation among EEA DPAs.
2. Facilitate cooperation between EDPB members and DPAs in third countries.
3. GDPR and LED transfer mechanisms.

GDPR Enforcement Reform

- In July 2023, the European Commission proposed the GDPR Procedure Regulation.
- Creates new procedural rules for **authorities when applying the GDPR** in cases which affect individuals located in more than one Member State.
- The text is still being negotiated.

- On April 10, 2024, the European Parliament adopted its position.
- Companies have raised concerns about some of the amendments:
 - Reduced confidentiality and business secret protections e.g., claimants could have access to the unredacted case file
 - Allows for DPAs to share information gathered during an investigation with other EU and national regulators e.g., DSA or AI regulators.
 - Limited incentives for complainant to reach an amicable settlement.



Brussels, 4.7.2023
COM(2023) 348 final
2023/0202 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679

New Enforcement Landscape

New EU Regulation	Relevant to	Primary regulator	Additional regulators involved
Digital Services Act	“Intermediary services”, i.e., conduit, caching, and hosting services (including online platforms & search engines)	One or more national authorities , coordinated by one Digital Services Coordinator	European Commission (EC) is responsible for Very Large Online Platforms and Very Large Online Search Engines (designated by EC)
Digital Markets Act	Designated gatekeepers and core platform services (CPS) (currently there are 6 gatekeepers and 22 CPS)	EC	NA – only the EC is responsible for enforcing the DMA
AI Act	Providers and deployers of AI systems and providers of general-purpose AI models	National authorities , one market surveillance authority and one notified body	EU AI Office is responsible for enforcing requirements for general-purpose AI
Data Act	Manufacturers of connected products and related services, data holders (make data available to recipients in the EU), cloud service providers	One or more national authorities , coordinated by Data Coordinator	Data protection authorities are responsible for enforcing provisions of the Data Act that relate to personal data

New Enforcement Landscape - Considerations



Complex question of regulators' competencies in cross-border scenarios.

There appears to be no clear one-stop-shop or main establishment mechanisms, such as under GDPR, in the acts. Potentially regulators in many EU countries will have competence.



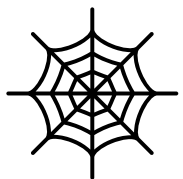
Varied interpretations can create tension and inconsistencies.

Interpretations of the new acts may vary between countries. This will create challenges for companies operating in multiple EU countries and may cause tensions with the GDPR e.g., the interpretation of profiling for the purposes of GDPR and DSA requirements.



Increased transparency increases the information available to other regulators e.g., DPAs.

Some acts e.g., DSA and DMA require companies to publish transparency reports, which could provide grounds for other authorities e.g., DPAs, to ask more questions.



Complex web of regulators competent for digital services.

In addition to many new laws, multiple regulators within each EU country are responsible for enforcement of the same acts. It is an increasingly complex regulatory landscape for international companies doing business in the EU navigate.

Questions for Discussion

- ① Will litigation become more likely in the future? If so, which topics will be most likely targets of litigation?
- ② Will the GDPR Procedure Regulation address the current challenges with GDPR enforcement from the company's perspective?
- ③ Is the EDPB going too far with its guidance and pushing the scope of its competence?
- ④ How can companies limit the enforcement risk with potentially many regulators having competency for overlapping issues under different acts?

Questions for Discussion



What areas of compliance do companies prioritize in light of evolving GDPR enforcement risks?



What documentation is most important to limit the risks when asked questions by a regulator or during an investigation?



How can privacy teams coordinate internally to ensure all public messaging about all matters related to personal data are consistent?



What are the biggest challenges companies face in relation to GDPR enforcement in the EU?

Thank you!