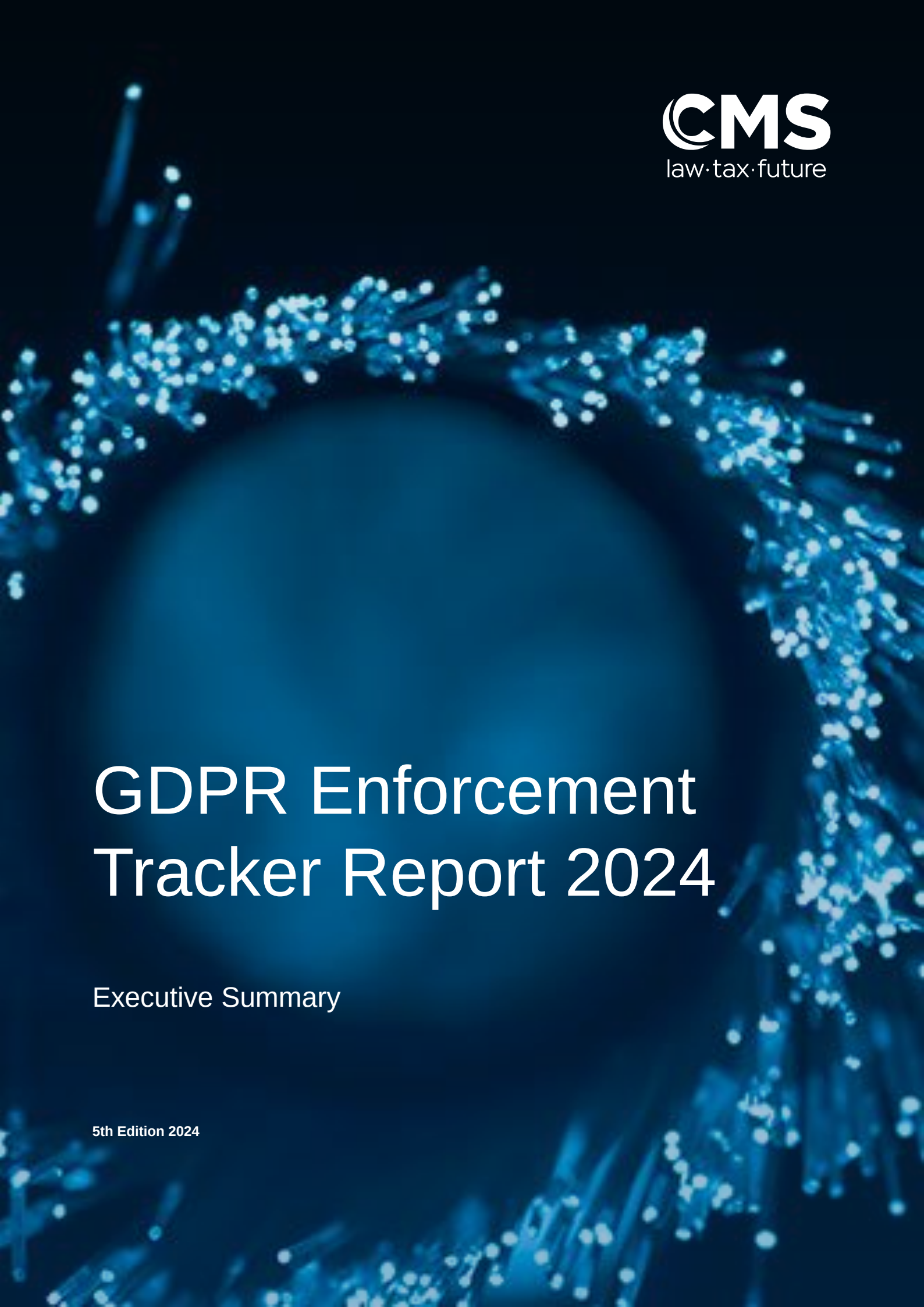


GDPR Enforcement Tracker Report 2024

Executive Summary

5th Edition 2024

Executive Summary – 2024

The CMS Data Protection Group is pleased to launch the fifth edition of the **GDPR Enforcement Tracker Report ("ET Report")**. This Executive Summary is our service for busy readers.

What the ET Report is all about

In the six years since the General Data Protection Regulation (GDPR) became applicable, its powerful framework for imposing fines has certainly helped to raise awareness and encourage compliance efforts – just as the European legislator intended. At the same time, the risk of fines of up to EUR 20 million or 4% of a company's global annual turnover can also lead to fear and reluctance or ignorance about compliance issues. We still believe that facts are better than fear.

The continuously updated list of publicly known GDPR fines in the **GDPR Enforcement Tracker** is our 24/7 remedy against fear. We started to extend our offering to the annual ET Report as a deep-dive approach five years ago. As in the previous editions, the ET Report is intended to provide you with more insights into the world of GDPR fines. Please find some remarks on the ET Report methodology at the very end of this Executive Summary.

What is new in the ET Report's fifth edition

This fifth edition of the ET Report covers all fines from 2018 to the editorial deadline of 1 March 2024. As at the editorial deadline of 1 March 2024, the Enforcement Tracker covered 2,225 fines (2,086 if only fines with complete information on the amount, date and controller are counted.)

The ET Report contains an overall summary on the existing fines in the "Numbers and Figures" section, followed by the "Enforcement Insights per business sector" (also including the overarching employment category) and the "Enforcement Insights per country" to provide background on the specific enforcement framework under national law.

Numbers and Figures

- Up to March 2024, a total number of 2,086 fines (+510 in comparison to the 2023 ET Report) were issued and recorded in the Enforcement Tracker (the database also includes cases with limited / no detailed information, leading to an overall total of 2,225 cases).

- We are aware that the different approach to the publication of fines / decisions is often rooted in national law, because (named) publication is a separate sanction in some jurisdictions (see also the **Enforcement Insights per country**). The European DPAs, nevertheless, have apparently agreed to publish aggregated case numbers at least annually, e.g. in their annual reports. Based on corresponding random samples, we already know that the actual number of fine cases is significantly higher than the number of cases recorded in the Enforcement Tracker.

- Total fines amount to around EUR 4.48 billion (+1.71 billion in comparison to the 2022 ET Report). In the whole reporting period 2018-2024, the average fine was around EUR 2.14 million across all countries. The higher average figures in comparison are mainly due to some massive fines against “Big Tech” imposed in 2021/2022 and the first fine in the billions in 2023.

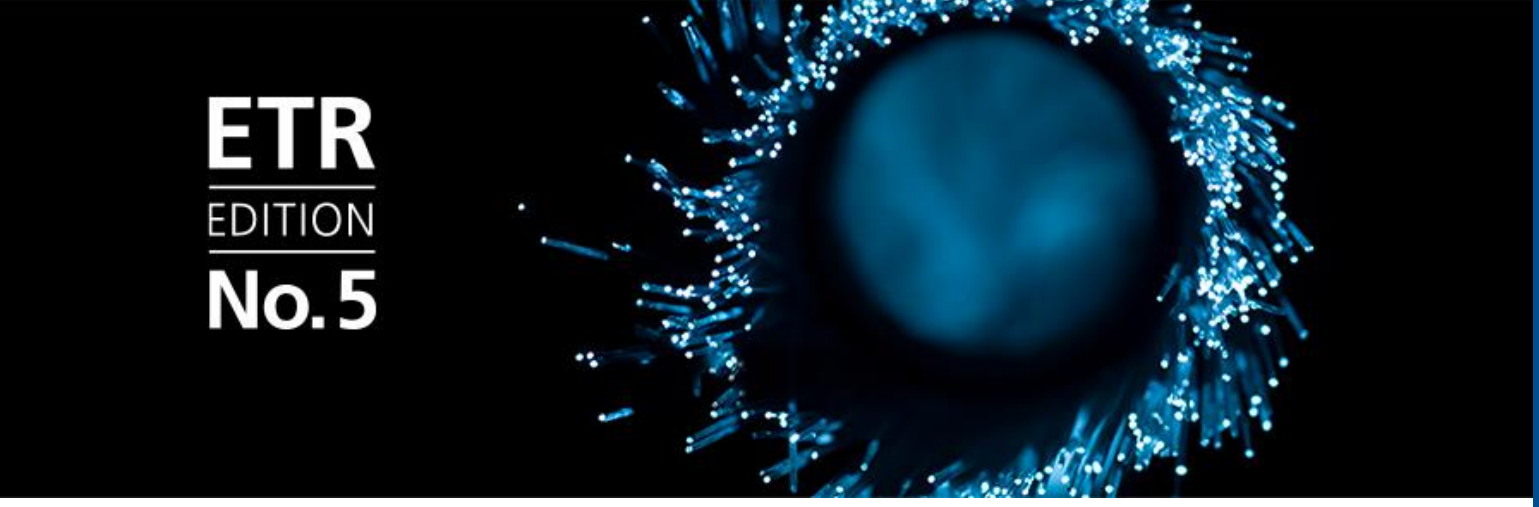
- The highest GDPR fine to date of EUR 1.2 billion was imposed by the DPA in Ireland in May 2023 due to the violation of regulations on international data transfers (**ETid-1844**). This is the first fine in the billions to date. The second highest fine by the DPA in Luxembourg (EUR 746 million, July 2021, **ETid-778**) and five Irish fines (EUR 405 million, September 2022, **ETid-1373**; EUR 390 million, January 2023, **ETid-1543**; EUR 345 million, September 2023, **ETid-2032**; EUR 265 million, November 2022, **ETid-1502** and EUR 225 million, September 2021, **ETid-820**) follow and dominate the top ten fines list.

- At the top of the list for types of violations in terms of number of fines and average amount are “insufficient legal basis for data processing” (612 fines, average EUR 2.7 million) and ”non-compliance with general data processing principles” (561 fines, average EUR 3.7 million). Next on the list is “insufficient technical and organisational measures to ensure information security” (357 fines, average EUR 1.1 million).

- Spain is – for the fifth consecutive year – leading the top list of numbers of fines per country by far, again followed by Italy and Romania. Ireland, Luxembourg, and France are leading the top lists for average fine amounts and total fine amounts per country, again reflecting the impact of the record fines imposed on big tech since 2021.

- The distribution of fines since May 2018 shows that the European supervisory authorities initially took a cautious approach in the first year of GDPR applicability with the first fine recorded in Portugal (EUR 400,000 against a public hospital in July 2018, **ETid-45**), followed by a relatively consistent and steadily increasing number of fines in 2018 and a ramp-up of enforcement between 2019 and mid-2021.

- Sanctions against "Big Tech" in 2022 and the first fine in the billions in 2023 catapulted the total amount of fines above EUR 4 billion.



Our overall takeaways

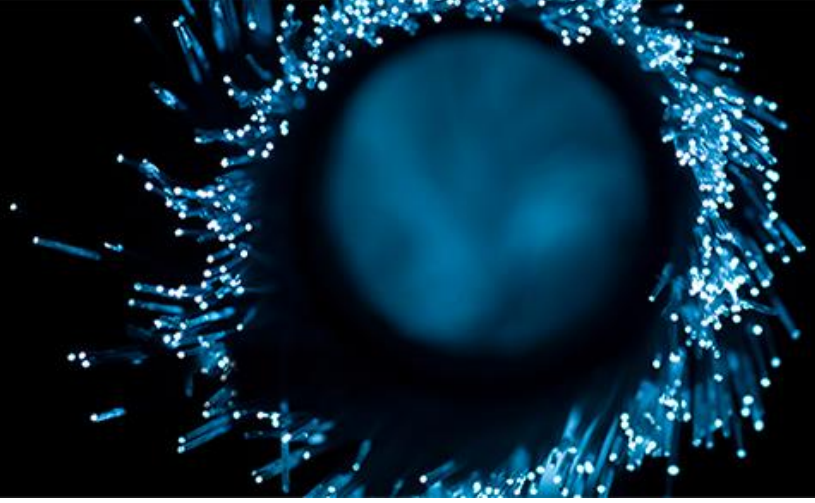
As we are aware that detailed research in the Enforcement Tracker may be burdensome, here are some overall takeaways:

- We have continued to stress this aspect for several years already, but it remains true over time: There are few areas of European data protection law more influenced by national laws and official practice than the GDPR fines. The administrative / sanctions law environment as well as an authority's position, personnel and tools, and finally its self-confidence / understanding of its own role appear to vary significantly between European countries – anything but fully harmonised. We have collected some further details in this respect in the **Enforcement Insights per country**.

- **Insufficient legal basis for data processing** and **non-compliance with general data processing principles** as well as **insufficient technical and organisational measures** are leading the "GDPR fine trigger" list and need to be on the organisational risk management radar. However, the "catch-all provision" on general data protection principles in Article 5 GDPR may be difficult to grasp, as the general principles cover all compliance requirements further detailed in the other, more specific provisions of the GDPR. The increasing number of Art. 5 GDPR fines may be the basis for a more detailed analysis in this respect.

- It goes without saying that **data subjects matter in data protection law**. Even without them being officially prioritised for GDPR compliance, it is fair to say that violations of data subjects' rights appear very likely to trigger fines.

- **Insufficient fulfilment of data subjects' rights** rank 4th in the list of violation types. Considering the complexity of dealing with, e.g., data subjects' access requests and transparency obligations, the importance of data subject-facing cases of non-compliance should lead to special emphasis on corresponding internal processes, policies and training. The focus on data subjects is – regardless of any obligations under data protection law – also a relevant issue in the 'digital aspects' of ESG (Environmental, Social & Governance) concepts, most notably for **Corporate Digital Responsibility** (CDR).



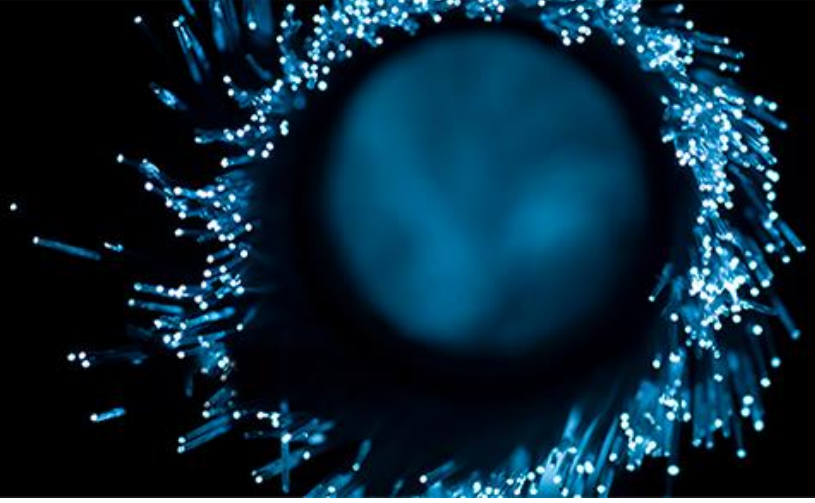
- Recognising the complexity of handling data subject access requests and transparency obligations, the European Data Protection Board (EDPB), as the **independent coordinating body of the European authorities** has made the right of access under Art. 15 GDPR the focus of its **2024 Coordinated Enforcement Action**.

- Recent rulings by the Court of Justice of the European Union (CJEU) have further clarified the scope of data subjects' right of access (e.g. **C-154/21**, **C-487/21** and **C-579/21**). While these rulings provide much-needed **clarity**, they also represent a tightening of data protection requirements for companies and as such diminish the leeway for companies to interpret Art. 15 GDPR in a data protection-friendly manner.

- **Sector exposure** is highest in **media, telecoms and broadcasting** and **industry and commerce** for the fourth consecutive year. Although the sector cases differ, we make the educated guess that B2C businesses are more likely to be subject to DPA investigations (and eventually to fines): greater "proximity" to data subjects may contribute to this as well as the latter's **willingness to bring (alleged) breaches of law to the attention of a DPA more quickly**.

- Another trigger could be the **use of new technologies**, which is encouraged by the constant pressure to innovate in these industries, such as the increasing development of AI. These systems can involve large-scale and complex processing of personal data and increase the likelihood of "risky" processing and potential violations of data protection.

- The riskier an innovative technology may be for the "rights and freedoms of data subjects", the more important it is for **appropriate risk management to delve into the details** (and corresponding documentation). For these purposes, it is necessary to **perform an extensive factual, legal and technical assessment before designing and implementing innovative technology**.



- The EDPB is well aware of this, stating in its **strategy for 2024-2027** that it will continue to face the challenges of new technologies such as artificial intelligence:

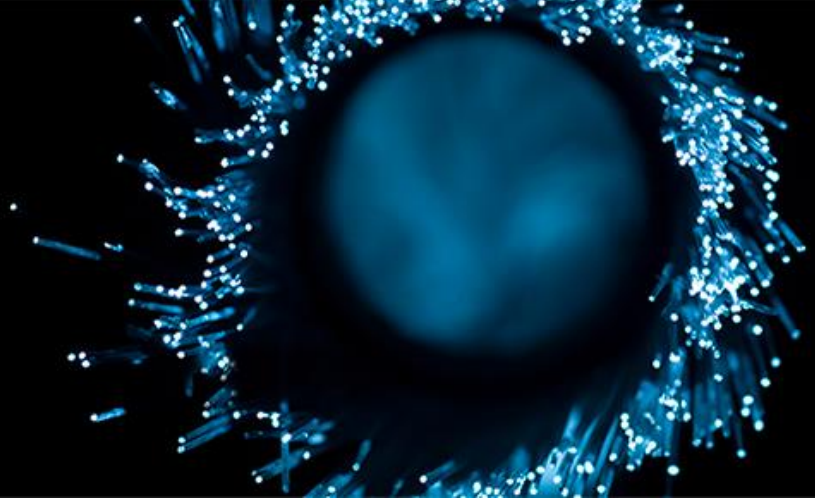
  "We will continue to monitor and assess new digital technologies to promote a humancentric approach, including those relating to, among others, Artificial Intelligence and digital identity. We will continue to issue guidance, where necessary, on the data protection implications of new technologies, and the correct application of the GDPR in the fast-developing digital landscape. This guidance will, among other things, include a further focus on the implementation of data protection concepts and principles in the context of new technologies, in particular in areas with significant risks for data subjects or where the data subjects belong to a particularly vulnerable group, such as children."

- However, the restriction on the operation of a generative AI provider by the Italian DPA has shown that data protection law already provides for an actual legal framework and actual enforcement options applicable to new technologies.

- Six years after the GDPR came into force, the European sanctions landscape has matured, but many questions still remain unanswered. Key questions on the interpretation of GDPR provisions, including those on fines, are increasingly the subject of court proceedings, with cases now reaching the CJEU.

- The CJEU was particularly active in 2023, issuing landmark decisions, such as in cases **C-683/21** and **C-807/21**, where it ruled **on the conditions under which national data protection authorities can impose fines on companies under the General Data Protection Regulation**.

- Judicial review of authority decisions is an essential pillar of rule-of-law principles – and decisions by DPAs (including enforcement notices or fining decisions) are no exception. The higher the stakes, the less inclined organisations are to immediately accept DPA decisions. As the number of data protection-related issues referred to and decided by the ECJ increases, judicial review of fines is also expected to rise. This trend promises to increase legal certainty in the interpretation of the GDPR.



- The **essential role of national supervisory authorities** and the **significant influence of national legislation** on fines and other sanctions procedures pose a challenge: The sometimes considerable differences in GDPR interpretation and enforcement between member states is difficult for companies to navigate. On the other hand, civil rights organisations complain about enforcement deficits (even referring to a "**GDPR crisis point**"), especially against big tech companies, for precisely this reason.

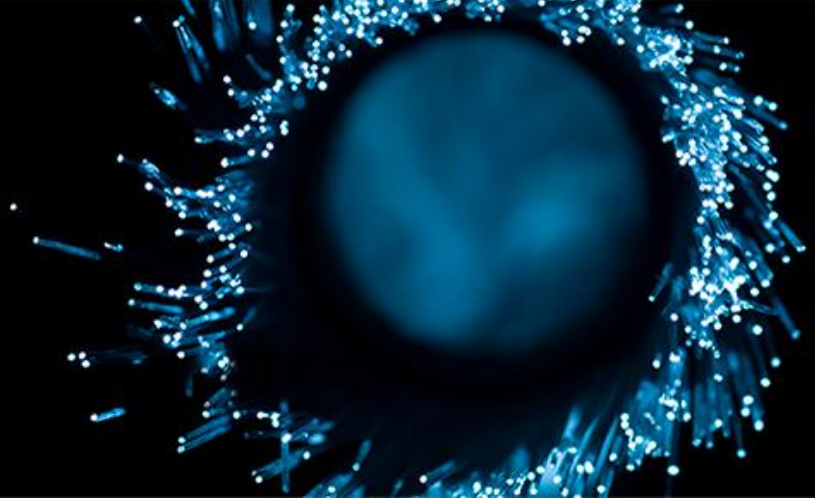
- This is exemplified by the recent practice of the Irish DPC, where significant fines, such as the record-breaking penalty against Meta of EUR 1.2 billion, were only imposed after a binding decision by the European Data Protection Board (EDPB).

- The EDPB, seems to be aware of this problem. Its **strategy for 2024-2027** focuses on "reinforcing a common enforcement culture and effective cooperation" as well as "enhancing harmonisation and promoting compliance":

  "The EDPB will further strengthen the efforts to ensure effective enforcement by, and cooperation between, the members of the EDPB. The EDPB will continue to support the development of cooperation and enforcement tools, and the sharing of expertise to increase the robustness of our common procedures, methodologies and decisions."

  "Following the EDPB's existing guidance on the key concepts of EU data protection law, we will further enhance our efforts to achieve a consistent application and effective enforcement of the law."

- In the meantime, you may wish to jump to the **Enforcement Insights per country section** to learn more about different procedural details in various jurisdictions – and reach out to your trusted legal advisor to assess your chances if the worst-case scenario of a GDPR fine has materialised.



- The temporary restriction of the generative AI application in Italy shows that **other types of sanctions** could also become more important in the future. These types of corrective measures may in some cases have an even greater impact on a company's business operations than a fine.
- At the same time, the possibilities of asserting the individual rights of data subjects are increasing, for example through class actions by consumer protection associations or statutory options for collective damage class actions. This is supported by a **CJEU ruling in 2022** in which the CJEU found that the GDPR does not preclude national legislation that allows a consumer protection association to take legal action against the controller allegedly responsible for a breach of data protection law without a mandate and regardless of the violation of specific rights of the data subjects.
- Besides, with the **Representative Actions Directive ((EU) 2020/1828)** now being implemented across the EU and many Member States having adapted their national procedural law to allow qualified entities to bring representative actions, we expect a further increase in the coming years.
- Companies must therefore increasingly expect to be sued by consumer associations for possible data protection violations.
- The European Commission will publish its **review of the General Data Protection Regulation in 2024** that builds on the report published in 2020. It remains to be seen what results and changes will emerge. **In any case, GDPR enforcement will continue to keep privacy pros busy for the next six years – and most likely beyond…**

Enforcement Insights per business sector

Finance, insurance and consulting

The increase of fines in the finance, insurance and consulting sector (already observed over the last years) continues. Further, the amount of imposed fines has increased with five fines exceeding EUR 1 million during the reference period of the 2024 ETR compared to one fine exceeding EUR 1 million during the reference period of the 2023 ETR.

The highest fines have all been imposed due to a lack of adequate internal compliance measures to ensure a sufficient legal basis for the processing of customer data. In each case, the controllers had failed to obtain effective consent for the data processing. Therefore, businesses in the finance, insurance and consulting sector should firmly establish and implement comprehensive processes to ensure a clear legal basis for each data processing activity. In particular, they should put in place adequate mechanisms to obtain – in absence of a statutory basis – effective consent from their customers where necessary and to ensure that data is only processed in accordance with this consent. In addition, authorities seem to look more closely at how exactly consent was obtained and whether data subjects were fully informed by the controller.

Moreover, insufficient data security measures resulted in significant fines and might also cause considerable reputational damage. Accordingly, companies operating in the financial and insurance sectors as well as consulting companies should focus on strong data security measures.

As digitalisation advances in the finance, insurance and consulting sector and more and more services are provided online or via apps, data security will become even more important. This is especially true as these companies operate in a highly regulated environment and are therefore subject to strict scrutiny regarding their data security and general IT security, not only by DPAs but also by financial regulators.

Accommodation and hospitality

The accommodation and hospitality sector includes global players as well as the café or B&B next door, and this diversity of the sector is reflected in this year's findings:

Almost 90% of the total fine amount can be attributed to two larger cases with six-figure fines (involving larger operators), with fines against SME being generally significantly lower. As in the previous years, operation of CCTV still plays a relevant role for this sector, making up more than 60% of all cases.

Healthcare

As we have already observed in recent years, most healthcare sector fines result from technical and organisational data protection deficiencies (e.g. lack of access restrictions for employees). This remained a common issue across many healthcare institutions and without a particular regional focus.

The reported cases indicate that compliance risk may be related to the (un-) availability of data (in addition to confidentiality as the most common security concern), migration of health data between systems and unintentional disclosure of health data (e.g., by indicating the sender on mail envelopes).

Finally, it is noteworthy that – as in the past year –, the Italian DPA has been particularly active in the field of healthcare and Covid-19-related violations remained relevant even in 2023.

Industry and commerce

The industry and commerce sector has faced significant fines for non-compliance with general data protection principles and insufficient legal basis for data processing. DPAs have shown their willingness to impose fines in the seven to eight-figure range. As far as the general principles of data processing are concerned, DPAs are closely reviewing the necessity of data processing and the duration of retention periods. The Clearview AI case shows that DPAs from different countries are willing to investigate and impose a significant fine for a single violation if it affects data subjects under their respective jurisdictions. It is worth noting that the Spanish DPA (aepd) is by far the most active authority, imposing more than 40% of all fines in this sector.

Real estate

Businesses in the real estate sector frequently perform “high risk” processing activities – ranging from processing prospective tenants' ID documents or detailed financial in-formation to operating CCTV systems (often by data processors/service providers) to protect property against theft, vandalism and similar problems. The implementation of adequate technical and organisational measures is key, as is a special focus on general processing principles such as data minimisation or limited retention. If publications of any kind are required, care should also be taken to ensure that personal data is not inadvertently disclosed, e.g. through pictures of individuals in rental offers.

Media, telecoms and broadcasting

Most GDPR fines in the media, telecoms and broadcasting sector were imposed because personal data were processed without sufficient legal basis. Also it can be observed that the supervisory authorities are imposing increasingly higher fines.

Moreover, record fines against Meta remain a recurring topic in this reporting period. The Irish DPA (DPC) fined Meta Platforms Ireland Limited with the highest fine to date of EUR 1.2 billion in May 2023 for violating the regulations on international data transfers. It is striking that the fine was only imposed by the DPC after a binding decision by the European Data Protection Board (EDPB), as has already been the case with other major fines imposed by the DPC in recent years.

The total amount of fines imposed is significantly higher than in the previous period, with an increase of 94%. This is of course partly due to the record fine imposed on Meta, however, other fines in the eight and even nine-digit range were imposed.

It is also worth noting that, unlike in previous years, the significant fines were spread across more different companies and not just on the same few players.

Transportation and energy

The number of cases in the transportation and energy sector has increased in recent years. On the other hand, the average fine amount has decreased. In particular, the amount of data subjects involved and the severity of the single violations, as well as the willingness to cooperate with the respective DPA, have represented important fac-tors in determining the amount of the fines. Despite the slight decrease in average fines, however, individual fines in the seven and even eight-figure range were imposed in this reporting period.

Insufficient legal basis for data processing and non-compliance with general data processing principles resulted in significant fines and were one of the most common rea-sons for the fines in the transportation and energy sector.

Public sector and education

Public authorities have a special position of trust that requires particularly strict compliance with data protection laws and an exceptionally high level of data security. The same applies to schools and other educational institutions, in particular those that process personal data of minors. DPAs appear to have increased scrutiny of the public and education sector since the last ET Report, notably in connection with the use of technology.

As in the previous year, DPAs still continued to impose fines due to Covid-19-related data protection violations this year. Further, the number of fines with regard to the processing of sensitive data (e.g. health data), profiling and tracking or surveillance of individuals continues to grow. It seems likely that this trend will continue in the future. In this context, it is notable that the highest and the second highest fines in the public and education sector (both imposed in 2022) result from an extensive and systematic collection and processing of personal data (including sensitive data) of citizens, mainly for statistical and profiling purposes.

Individuals and private associations

If one goes by public perception, the GDPR seems to be aimed primarily at “digital global players”. The analysis of the Individuals and private associations sector, how-ever, paints a slightly different picture:

While the number of fines in this area has not risen as significantly this year as in the previous year, there has still been an increase of more than 50%, while the total amount has only increased slightly. This indicates that many small fines were imposed on individuals. More than half of all known fines in this area were imposed by the Spanish DPA (193).

DPAs tend to treat bigger non-profits (esp. sports associations) just like similarly sized businesses. They imposed fines for various offences ranging from lack of technical and organisational measures to insufficient information provided to data subjects.

As far as individual entrepreneurs and private individuals are concerned, the DPAs seem to pay very close attention to the extent to which the violation was foreseeable by the individual and to the motives for the processing. The number of data subjects and the violator's intention to pursue economic interests through the illegal data processing was particularly important.

Blending into an overall trend and emphasising a focus on intrusive processing activities, nearly half of all fines in this sector were based on illegal video surveillance / CCTV. This underlines the prevailing focus of data protection authorities on video surveillance, as they consider video surveillance to be such a high-risk form of processing that strict requirements must be met, even by private individuals.

Employment

We have noticed a significant increase in the total amount of fines imposed to date, mainly due to an eight-figure fine imposed during this reporting period.

Despite the fact that fines of this amount are currently still the exception rather than the rule, we still assume that the protection of employee data will remain a key field of activity for DPAs, considering the overall importance of employee data processing for companies of any size and in any sector.

From a legal perspective, employees are considered to be particularly vulnerable. Moreover, employment courts are paying stricter attention to whether evidence presented by employers in employment court proceedings is admissible or must be dis-regarded due to violations of data protection laws during its gathering.

Employees may be more likely to raise complaints with a DPA, especially in case of conflict situations. Cases ultimately brought before employment courts can additionally include claims for damages based on data protection violations.

In our experience, employers have had to justify their data protection compliance not only to DPAs but also to trade unions and/or works councils in recent years. Employees and co-determination bodies are increasingly exploiting employers' uncertainties about data protection to assert other legal positions against employers.

At the same time, cases involving the processing of employee data remain legally complex: the processing of personal data in the employment context is closely linked to the national legal framework governing the employment relationship, and the established interpretation of such national employment laws usually influences the permitted extent of employee data processing. This aspect leads to a challenge especially for international organisations, frequently trying to apply uniform HR data processing policies across global organisations and/or operating integrated HR management systems, requiring increased compliance efforts.

An initial analysis of employee data-related fines indicates that employers' reliance on a statutory legal basis (such as performance of a contract) for their data processing may be the best choice. Employee consent remains – due to the assumed structural imbalance between employers and employees – limited to individual, specific cases in which employees have a "real choice".

ET Report Methodology

In addition to our necessary focus on publicly available fines, there are some other inherent limits to the data behind this whole exercise. Please find some fine print in our more **detailed remarks on methodology**.

What's next?

The Enforcement Tracker Report and the Enforcement Tracker are a living project. While the sixth edition of the ET Report will be published in one year's time (around May 2025), we highly appreciate any form of feedback and want to thank everybody who has reached out to us so far while the data protection landscape is quickly evolving on a global scale and interfaces between national/regional concepts are developing even in absence of a global data protection law.

We interacted with peers from the legal profession, privacy professionals with a more advanced tech background as well as researchers from various disciplines.

We strongly encourage you to continue with this interaction (info@enforcementtracker.com). And we apologise in advance if our feedback may take some more time: The data protection world has not calmed down, and this may go on for a while.

Enforcement Tracker Report 2024

Enforcement Tracker Report Key Editors

Christian Runte
Partner
E christian.runte@cms-hs.com

Dr. Anna Lena Füllsack, M.A.
Senior Associate
E annalena.fuellsack@cms-hs.com

Dr. Alexander Schmid
Senior Associate
E alexander.schmid@cms-hs.com

Luiza Esser
Research Associate
E luiza.esser@cms-hs.com

Enforcement Tracker Core Team

Luiza Esser, Alexander Schmid
E info@enforcementtracker.com

CMS Data Protection Contacts

Albania
Mirko Daidone
E mirko.daidone@cms-aacs.com

Algeria
vacant (new contact to be confirmed)

Angola
Luís Borba Rodrigues
E luis.borbarodrigues@lbr-legal.com

Austria
Johannes Juranek
E johannes.juranek@cms-rrh.com

Belgium
Tom de Cordier
E tom.decordier@cms-db.com

Bosnia and Herzegovina
Sanja Voloder
E sanja.voloder@cms-rrh.com

Brazil
Ted Rhodes
E ted.rhodes@cms-cmno.com

Bulgaria
Nevena Radlova
E nevena.radlova@cms-cmno.com

Gentscho Pavlov
E gentscho.pavlov@cms-rrh.com

Chile
Diego Rodriguez
E diego.rodriguez@cms-ca.com

China
Nick Beckett
E nick.beckett@cms-cmno.com

Ulrike Glueck
E ulrike.glueck@cmslegal.cn

Colombia
Lorenzo Villegas-Carrasquilla
E lorenzo.villegas@cms-ra.com

Croatia
Marija Zrno
E marija.zrno@cms-rrh.com

Czech Republic
Tomas Matějovský
E tomas.matejovsky@cms-cmno.com

France
Anne-Laure Villedieu
E anne-laure.villedieu@cms-fl.com

Germany
Christian Runte
E christian.runte@cms-hs.com

Hong Kong
Jonathan Chu
E jonathan.chu@cms-cmno.com

Hungary
Dóra Petrányi
E dora.petranyi@cms-cmno.com

Italy
Italo de Feo
E italo.defeo@cms-aacs.com

Kenya
Julius Wako
E julius.wako@cms-di.com

Luxembourg
Vivian Walry
E vivian.walry@cms-dblux.com

North Macedonia
Marija Filipovska
E marija.filipovska@cms-rrh.com

CMS Data Protection Contacts

Mexico
César Lechuga Perezanta
E cesar.lechuga@cms-wll.com

Monaco
Daniel Goldenbaum
E daniel.goldenbaum@cms-pcm.com

Montenegro
Dragana Bajić
E dragana.bajic@cms-rrh.com

Netherlands
Erik Jonkman
E erik.jonkman@cms-dsb.com

Norway
Ove André Vanebo
E ove.vanebo@cms-kluge.com

Oman
Ben Ewing
E ben.ewing@cms-cmno.com

Peru
Ramon Huapaya
E ramon.huapaya@cms-grau.com

Poland
Tomasz Koryzma
E tomasz.koryzma@cms-cmno.com

Portugal
José Luís Arnaut
E joseluis.arnaut@cms-rpa.com

Romania
Cristina Popescu
E cristina.popescu@cms-cmno.com

Serbia
Dragana Bajić
E dragana.bajic@cms-rrh.com

Saudi Arabia
Ben Gibson
E ben.gibson@cms-cmno.com

Singapore
Sheena Jacob
E sheena.jacob@cms-holbornasia.com

Slovakia
Martina Simova
E martina.simova@cms-cmno.com

Oliver Werner
E oliver.werner@cms-rrh.com

Slovenia
Amela Žrt
E amela.zrt@cms-rrh.com

South Africa
Zaakir Mohamed
E zaakir.mohamed@cms-rm.com

Spain
Javier Torre de Silva
E javier.torredesilva@cms-asl.com

Switzerland
Dirk Spacek
E dirk.spacek@cms-vep.com

Turkey
Alican Babalioglu
E alican.babalioglu@cms-cmno.com

Döne Yalçın
E doene.yalcin@cms-rrh.com

Ukraine
Olga Belyakova
E olga.belyakova@cms-cmno.com

Maria Orlyk
E maria.orlyk@cms-rrh.com

United Arab Emirates
Ben Gibson
E ben.gibson@cms-cmno.com

United Kingdom
Emma Burnett
E emma.burnett@cms-cmno.com