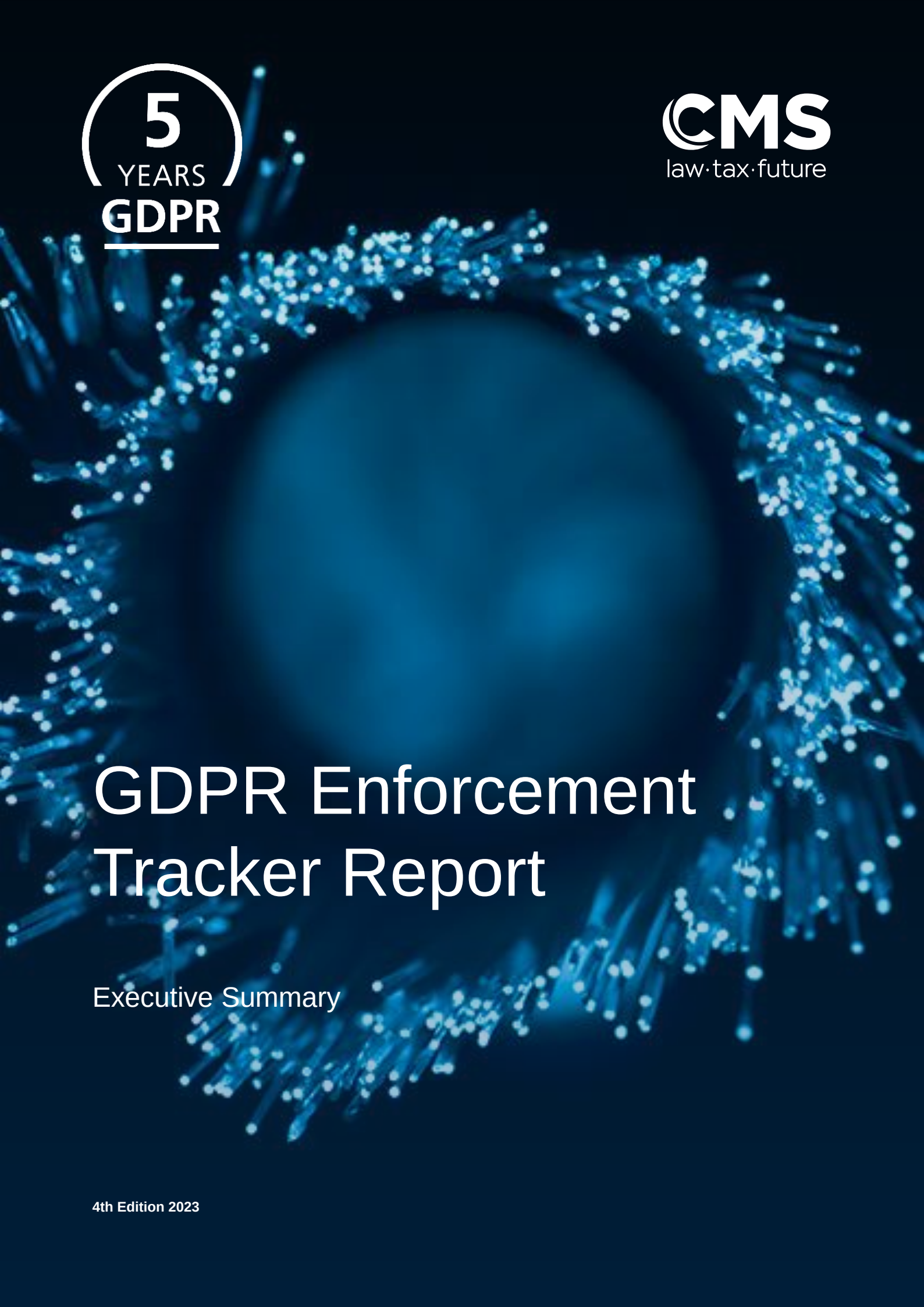


GDPR Enforcement Tracker Report

Executive Summary

4th Edition 2023

A warm welcome…

…to the fourth edition of the GDPR Enforcement Tracker Report (“ET Report”) – the anniversary edition celebrating five years of GDPR. This Executive Summary is our service for busy readers (somebody told us that privacy professionals’ schedules are overflowing almost constantly since 2018), and also printable for bedside reading without a digital device. The full ET Report is an online-only publication available here.

What the ET Report is all about

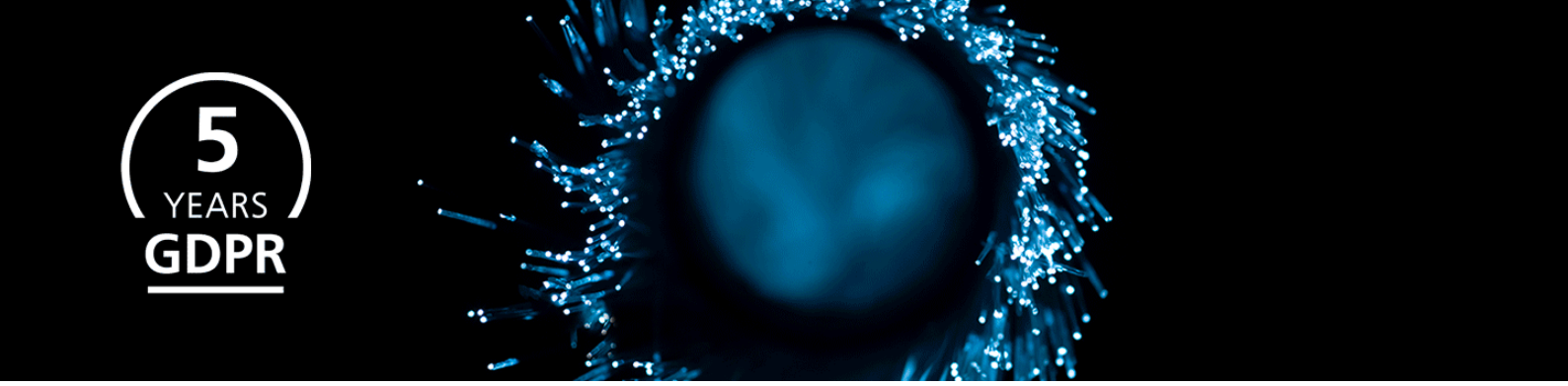
In the five years since the General Data Protection Regulation (GDPR) became applicable its powerful framework for imposing fines has certainly helped to raise awareness and encourage compliance efforts – just as the European legislator intended. At the same time, the risk of fines of up to EUR 20 million 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 four years ago. As in the previous three 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 fourth edition

The fourth edition of the ET Report covers all fines listed in the Enforcement Tracker between 25 May 2018 and the ET Report’s editorial deadline on 1 March 2023. The anniversary edition is therefore based on around 1,672 Enforcement Tracker entries (1,576 if only fines with complete information on the amount, date, controller and reason for non-compliance 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.



Looking back five years – and watching GDPR enforcement mature…

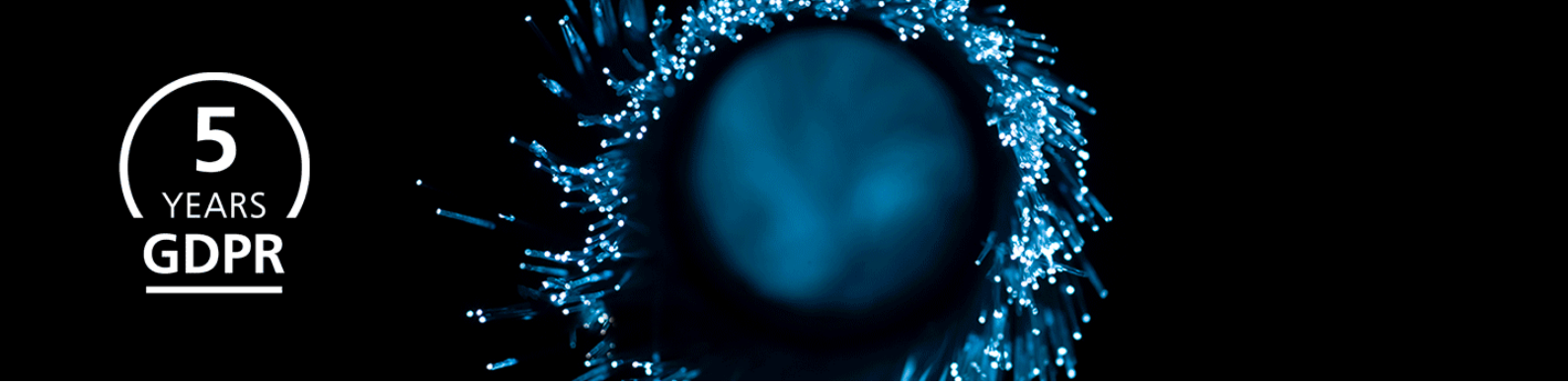
- The sanctions regime of the GDPR received attention even before the new data protection law was applicable: for the first time since the first steps towards harmonising European data protection law in the mid-1990s, the legislator provided for **tangible sanctions as a deterrent for non-compliance**.

- Five years later, we see a **European sanctions landscape** that has **already come of age**, but with **many questions remaining unanswered**. Relevant fundamental questions on the interpretation of the GDPR – including on fines – are the subject of legal proceedings and have in the meantime reached the European Court of Justice (ECJ). As an example, a decision in the "Deutsche Wohnen" case is expected soon, and on the basis of the Advocate General's opinion, the ECJ will decide on the possible strict liability of companies for data protection violations (spoiler: the Advocate General apparently rejects such strict liability), and other relevant ECJ decisions will follow.

- Notwithstanding this, the European **data protection authorities** have relatively **quickly begun to make use of their new authorities** under the GDPR: The first publicly known fine was imposed only two months after the GDPR became applicable (ETid-45), followed by other smaller cases in the following months of 2018. In January 2019, the French data protection authority provided the first landmark case with a fine of EUR 50 million against Google LLC (ETid-23), which still appears in the top ten list today.

- The years 2019 and 2020 were a **period of continuous GDPR enforcement** – the total number of cases rose steadily to several hundred, including some fines in the millions (e.g., ETid-186, ETid-187, ETid-189). At the same time the supervisory authorities were obviously **working on larger cases** that came to light during 2021: The DPA in Luxembourg imposed the highest GDPR fine to date in an amount of EUR 746 million (ETid-778) which led to the total amount of fines **exceeding the one billion euro mark** for the first time, followed by a French case in December 2021 with a EUR 90 million fine (ETid-978). The total number of **1,000 publicly known cases** was reached in January 2022 and the **total amount of two billion euros** was exceeded in autumn 2022, essentially due to several decisions by the Irish authority (EUR 405 million, September 2022, ETid-1373; EUR 390 million, January 2023, ETid-1543 and EUR 265 million, November 2022, ETid-1502).

- The statistical figures alone prove that the GDPR sanctions are **not just a theoretical risk**. A look at the more detailed analysis in the ET Report also shows that **sanctions are not limited to "big tech"** – numerous fines have also been imposed on small and medium-sized enterprises outside the technology sector.



- However, five years of experience with GDPR enforcement have also revealed problematic aspects. In particular, 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.

- The European Data Protection Board, as the independent coordinating body of the European authorities, seems to be aware of this issue: "Effective enforcement and efficient cooperation" between the national authorities is a focus of the work programme for 2023/2024.

- Finally, other types of sanctions may become more important in the future. The recent clash between Italy's Garante and the provider of a generative AI application in relation to the processing of personal data demonstrates that **corrective measures other than fines** – e.g., a temporary limitation of personal data processing – may have an even more relevant impact on a company's business operations. At the same time, the possibilities of asserting **individual claims for damages by data subjects** are increasing, for example through representative action by consumer protection associations or statutory options for collective damage class actions.

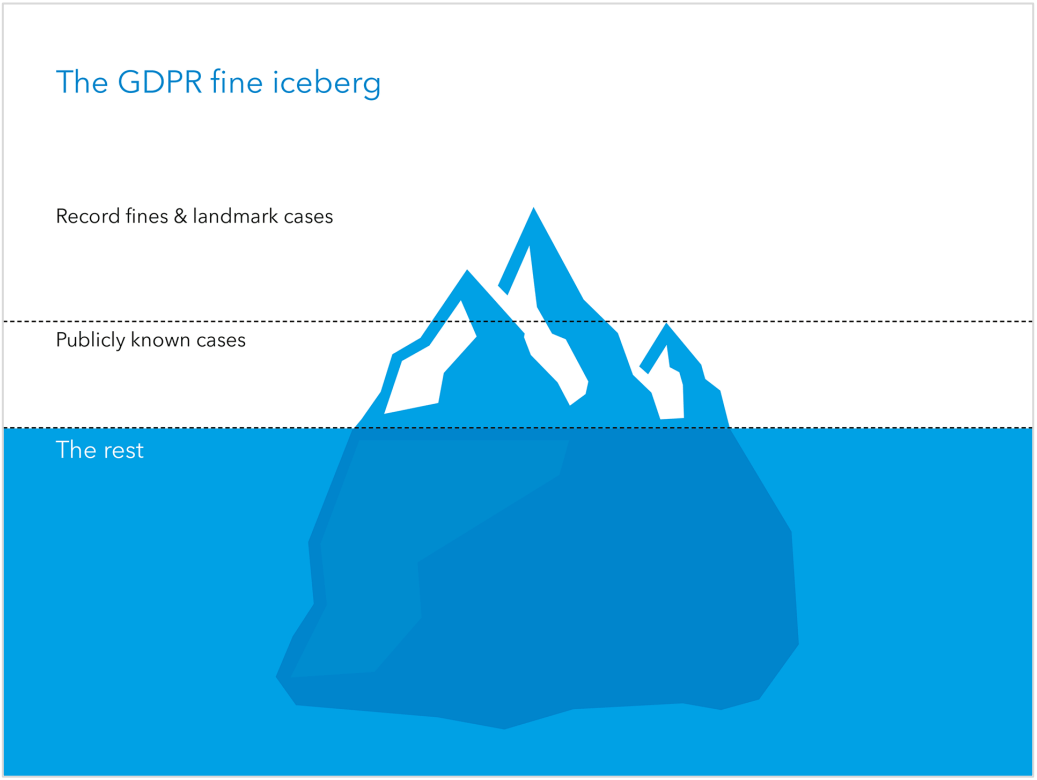
In any case, GDPR enforcement will continue to keep privacy pros busy for the next five years – and most likely beyond...

Numbers and Figures

- Up to March 2023, a total number of 1,576 fines (+545 in comparison to the 2022 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 1,672 cases).
- Total fines amount to around EUR 2.77 billion (+1.19 billion in comparison to the 2022 ET Report). In the whole reporting period 2018-2023, the average fine was around EUR 1.8 million across all countries. The higher average figures in comparison are mainly due to some massive fines against “Big Tech” imposed in 2021/2022.
- The highest GDPR fine to date of EUR 746 million was imposed by the DPA in Luxembourg in July 2021 due to non-compliance with general data processing principles (ETid-778). Four Irish fines (EUR 405 million, September 2022, ETid-1373; EUR 390 million, January 2023, ETid-1543; EUR 265 million, November 2022, ETid-1502 and EUR 225 million, September 2021, ETid-820) and a French case (approximately EUR 90 million, December 2021, ETid-978) 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” (495 fines, average EUR 0.9 million) and ”non-compliance with general data processing principles” (Art. 5 GDPR, 381 fines, average EUR 4.5 million). Next on the list are “insufficient technical and organisational measures to ensure information security” (279 fines, average EUR 1.3 million) and “insufficient fulfilment of data subjects' rights” (150 fines, average EUR 1.5 million).
- Spain is – for the fourth consecutive year – leading the top list of numbers of fines per country by far, again followed by Italy and Romania. Luxembourg, Ireland 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. While 2021 had already ended with high fines, massive sanctions against "Big Tech" in 2022 catapulted the total amount of fines above EUR 2 billion.

Our high-level takeaways

Looking back over the last five years of intense involvement with GDPR fines, we have only seen the tip and middle of the iceberg. The tip represents highly visible record fines and landmark cases such as those in our top 10 list. Below them – only visible with a closer look – are the other publicly known cases, i.e. those listed in the Enforcement Tracker. As with a real iceberg, however, the real danger can lurk beneath the surface of the water – that is where the "invisible" cases are found that are not published by DPAs or otherwise made public.



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.

While we are still working to shed more light on the invisible cases, we believe that it is valuable to look at the numerous cases beyond the already well-known record fines / landmark cases.

Even if the fines do not reach double- or triple-digit millions, the available information is often helpful for risk management purposes: What were the facts on which the fine was based? How did the case come to the attention of the DPA? What is the alleged violation of applicable law? Looking into the details of the cases often shows that controllers do not per se carry out unlawful data processing – frequently, otherwise permissible data processing is sanctioned due to its unlawful scope.

As we are aware that such 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 – and we noted that also the European Data Protection Board included a reference to "EC draft legislation aiming to harmonise administrative laws of the GDPR enforcement" in its work programme for 2023/2024. For the time being, organisations have to deal with a fragmented enforcement map (and are well advised to have local expertise at hand…).

- **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 Article 5 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 subject's rights appear very likely to trigger fines. **Insufficient fulfilment of data subject's rights and of information obligations** rank 4th and 5th 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).

- **Sector exposure** is highest in **media, telecoms and broadcasting** and **industry and commerce** for the third / second 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 (= higher likelihood of "risky" processing of consumer data) promoted by constant pressure to innovate in these business sectors.

- Also in this edition of the ET Report, we had to include various references to the **risks of monitoring persons**, perhaps most visible in relation to employee data processing. Although the focus of many cases is still on **video surveillance (CCTV)**, the criteria for the use of invasive means of surveillance could also be **relevant for other technical innovations**. 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 most relevant example for 'new technologies' (even in the 21st century…) may be **artificial intelligence (AI)**: Pending new and dedicated AI regulation, some examples – such as a recent case involving generative AI in Italy – have already demonstrated that **data protection law provides for an actual legal framework and actual enforcement options** applicable to new technologies.

- The recent generative AI case has shed light on yet another aspect: **Fines are far from the only possible consequence of non-compliance**. The supervisory authorities have a whole bundle of corrective powers at their disposal under Art. 58(2) GDPR – and, e.g., the "*temporary or definitive **limitation including a ban on processing***" may even have a **more significant effect** on a company than a fine.

- 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 more risks are at stake, the higher the probability that an organisation may not – or at least not immediately – accept a DPA decision**. In the same way that the number of data protection-related questions referred to and decided by the ECJ is on the rise, the judicial review of decisions imposing fines is also likely to increase – which will hopefully lead to an increase in legal certainty in the interpretation of the GDPR. 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.

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 – however, the amount of imposed fines has decreased: Only one fine during the last reference period exceeded EUR 1 million compared to the previous period with several fines ranging in the millions.

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 kebab stand 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. Operation of CCTV still plays a relevant role for this sector, making up more than 70% of all cases.

Healthcare

Healthcare sector fines result from technical and organisational data protection deficiencies and in particular inadequate (or lack of) access restrictions and access management systems. 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.

Industry and commerce

The industry and commerce sector was subject to significant fines for non-compliance with general data protection principles and insufficient data security measures. Also in this sector, DPAs have shown that they are willing to impose 6 or even 7-figure fines for insufficient technical and organisational measures, especially when large amounts of personal data are exposed to public access. In relation to general data processing principles, DPAs are closely examining the necessity of data processing and the length 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.

Real estate

Businesses in the Real Estate sector frequently perform “high risk” processing activities – ranging from processing prospective tenants' ID documents or detailed financial information 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.

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. Moreover, fines against Meta remain a recurring topic. Such cases also demonstrate that the consultation procedure set out in the GDPR has an important function, particularly in relation to the enforcement of the GDPR in Ireland. Without the relevant consultation and the final decision of the European Data Protection Board (EDPB), the case at hand would have been decided and sanctioned in a fundamentally different way. In addition, care must be taken to ensure that all transfers to third parties are subject to data protection law.

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 factors in determining the amount of the fines.

Insufficient legal basis for data processing and non-compliance with general data processing principles resulted in significant fines for companies in the transportation and energy sector. However, the number of fines for data security breaches was substantially lower in this sector. This could be due to the fact that the sector may have responded well to the strict monitoring of this issue by DPAs in previous years.

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 expected, the number of fines in connection with COVID-19-related data processing has increased further since the last ET Report. We consider it likely that even more COVID-19 related violations will be registered and sanctioned in the coming years. 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, however, paints a slightly different picture:

The number of fines for this sector has more than doubled compared to last year's ET Report, while the total amount has increased only modestly. This indicates that many small fines were imposed against individuals. More than half of all known fines in this sector were imposed by the Spanish DPA (114), followed by the German DPAs (43).

DPAs tend to treat bigger non-profits (esp. sports associations) just like similarly sized businesses. They imposed fines for various offenses 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, with a special focus on dashcams. This underscores the general focus of DPAs on video surveillance. They consider CCTV to be such a risky form of processing that strict requirements must be met even by private individuals.

Employment

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. Moreover, employment courts are paying stricter attention to whether evidence presented by employers in employment court proceedings is admissible or must be disregarded 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

We do not resort to witchcraft nor do we have preferential access to GDPR fine information (at least in most cases, but we are still working on that…) when we are busy in the Enforcement Tracker engine room and preparing the ET Report. 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 fourth edition of the ET Report will be published in one year's time (around May 2024), we highly appreciate any form of feedback (constructive is preferred…) and want to thank everybody who has reached out to us so far.

We received interesting thoughts, hints leading to forgotten fines (hidden deeply in remote corners of a supposedly completely captured world), recommendations for additional features (our list is growing steadily) as well as relevant contributions from stakeholders located outside Europe demonstrating that 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.

The people behind the ET Report

Editors in Chief | Heads of CMS Data Protection Group

Michael Kamps
Partner

E michael.kamps@cms-hs.com

Christian Runte
Partner

E christian.runte@cms-hs.com

ET Report Editors | Enforcement Tracker Core Team

Luiza Esser, Fiona Savary, Alexander Schmid
E info@enforcementtracker.com

Enforcement Insights per business sector

Christoph Ceelen, Huy Do Chi, Anna Lena Füllsack, Felix Glocker,
Katharina Hirzle, Martin Kilgus, Martin Krings, Kevin Leibold,
Arne Schmieke, Georg Schneider

Enforcement Insights per country

Tom de Cordier, Séverine Bouvy,
Anne-Laure Villedieu, Maxime Hanriot,
Italo de Feo, Mariangela Selvaggiuolo,
Erik Jonkman, Inge Hajema,
Ove Vanebo, Stian Hultin Oddbjoernsen,
Johannes Juranek, Christina Maria Schwaiger,
Tomasz Koryzma, Adriana Zdanowicz -Leśniak, Damian Karwala,
José Luis Piñar, Javier Torre de Silva, Miguel Recio,
Emma Burnett, Loretta Pugh,
Dóra Petrányi, Márton Domokos, Katalin Horváth,
Tomáš Matějovský, Daniel Szpyrc,
Eva Petrova, Maria Harizanova

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

Michael Kamps
E michael.kamps@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