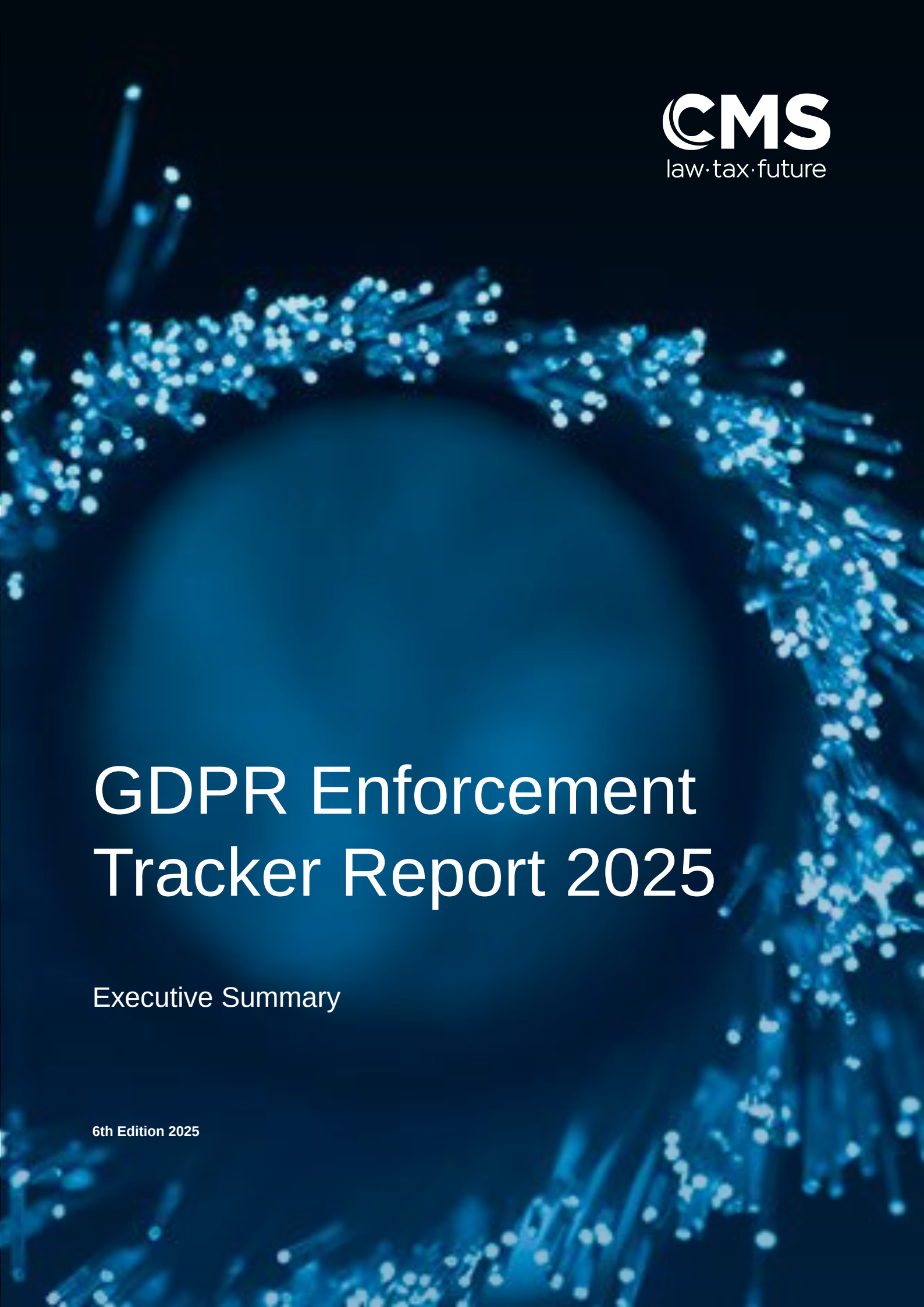


GDPR Enforcement Tracker Report 2025

Executive Summary

6th Edition 2025

Executive Summary – 2025

The CMS Data Protection Group is pleased to launch the sixth 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 seven 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 six 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 sixth edition?

This sixth edition of the ET Report covers all fines from 2018 to the editorial deadline of 1 March 2025. As of the editorial deadline of 1 March 2025, the Enforcement Tracker covered 2,560 fines (2,245 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 by Business Sector" (also including the overarching employment category) and the "Enforcement Insights by Country" to provide background on the specific enforcement framework under national law.

Numbers and Figures

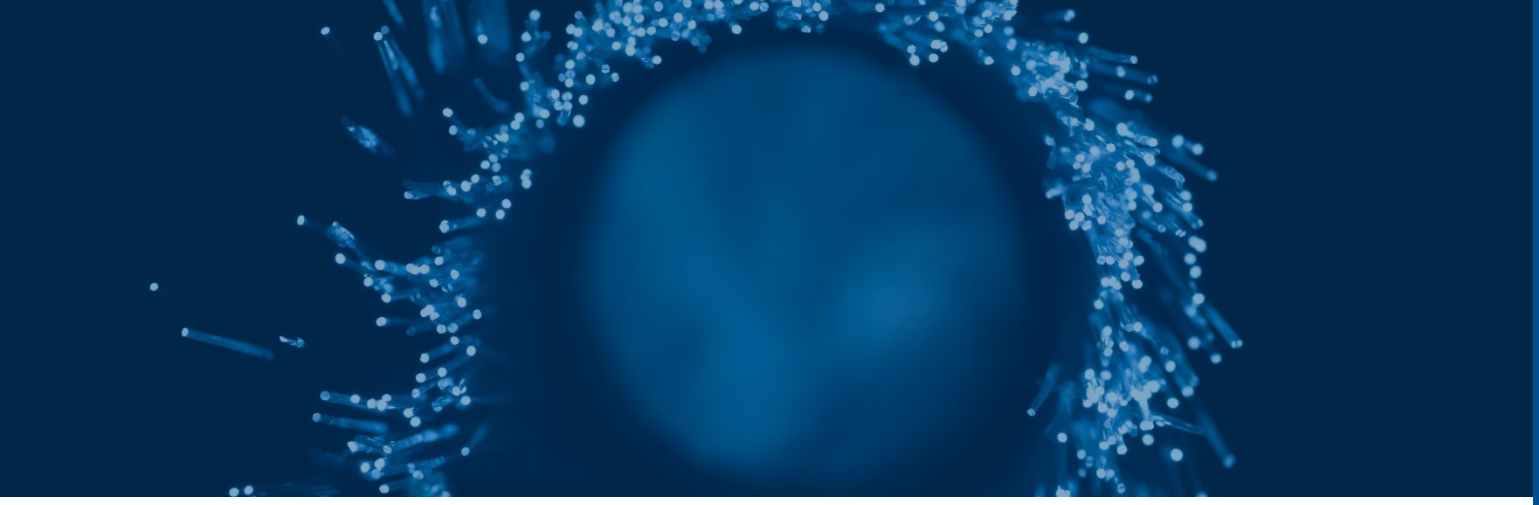
- Up to March 2025, a total number of 2,245 fines (+159 in comparison to the 2024 ET Report) were issued and recorded in the Enforcement Tracker (the database also includes cases with limited/no detailed information, leading to an overall total of 2,560 cases).
- We are aware that the different approach 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 by 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 exceeded the five-billion mark for the first time and amount to around EUR 5.65 billion (+EUR 1.17 billion in comparison to the 2024 ET Report). In the whole reporting period 2018-2024, the average fine was around EUR 2.36 million across all countries (+EUR 0.22 million in comparison to the 2024 report).
- 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**), seven Irish fines (EUR 405 million, September 2022, **ETid-1373**; EUR 390 million, January 2023, **ETid-1543**; EUR 345 million, September 2023, **ETid-2032**; EUR 310 million, October 2024, **ETid-2469**; EUR 265 million, November 2022, **ETid-1502;** EUR 251 million, December 2024, **ETid-2484** and EUR 225 million, September 2021, **ETid-820**) and one fine from the Netherlands (EUR 290 million, July 2024, **ETid-2447**) follow and make up the top ten fines list.

- At the top of the list of types of violations in terms of number of fines and average amount are “insufficient legal basis for data processing” (669 fines, average EUR 2.9 million) and “non-compliance with general data processing principles” (644 fines, average EUR 3.8 million). Next on the list is “insufficient technical and organisational measures to ensure information security” (418 fines, average EUR 2.0 million).

- Spain is – for the sixth consecutive year – far in the lead on the list of numbers of fines by country, again followed by Italy and Romania. Ireland, Luxembourg and the Netherlands are in the lead on the list of average fine amounts and total fine amounts by 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. Whereas the current reporting period brought the total fine amount above the five billion mark, the European authorities appear to have entered a “business as usual” period with limited landmark cases.



Our overall Takeaways

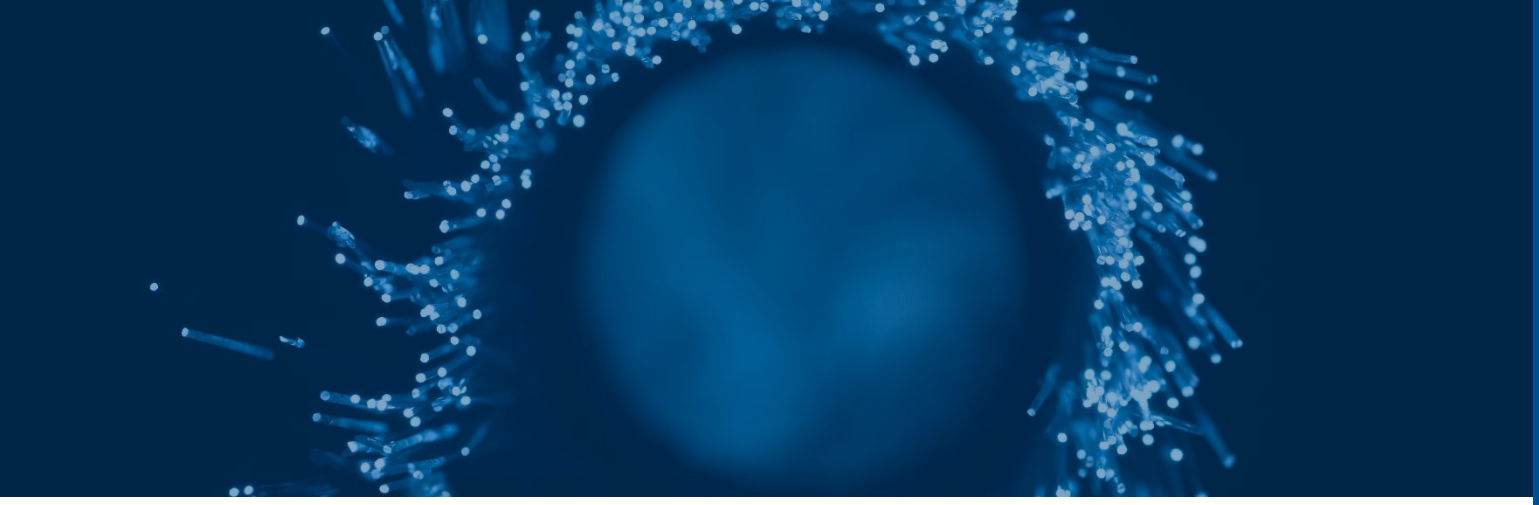
As we are aware that detailed research in the Enforcement Tracker may be burdensome, here are some overall takeaways:

- We have continued to stress this aspect for several years already, but it remains true to this day: 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 – demonstrating that practices are anything but fully harmonised. We have collected some further details in this respect in the **Enforcement Insights by Country** section.

- **Insufficient legal basis for data processing and non-compliance with general data processing principles as well as insufficient technical and organisational measures** lead 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** ranks fourth in the list of violation types. Considering the complexity of dealing with, e.g. data subjects' access requests and transparency obligations, the importance of cases of non-compliance at the cost of data subjects 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).

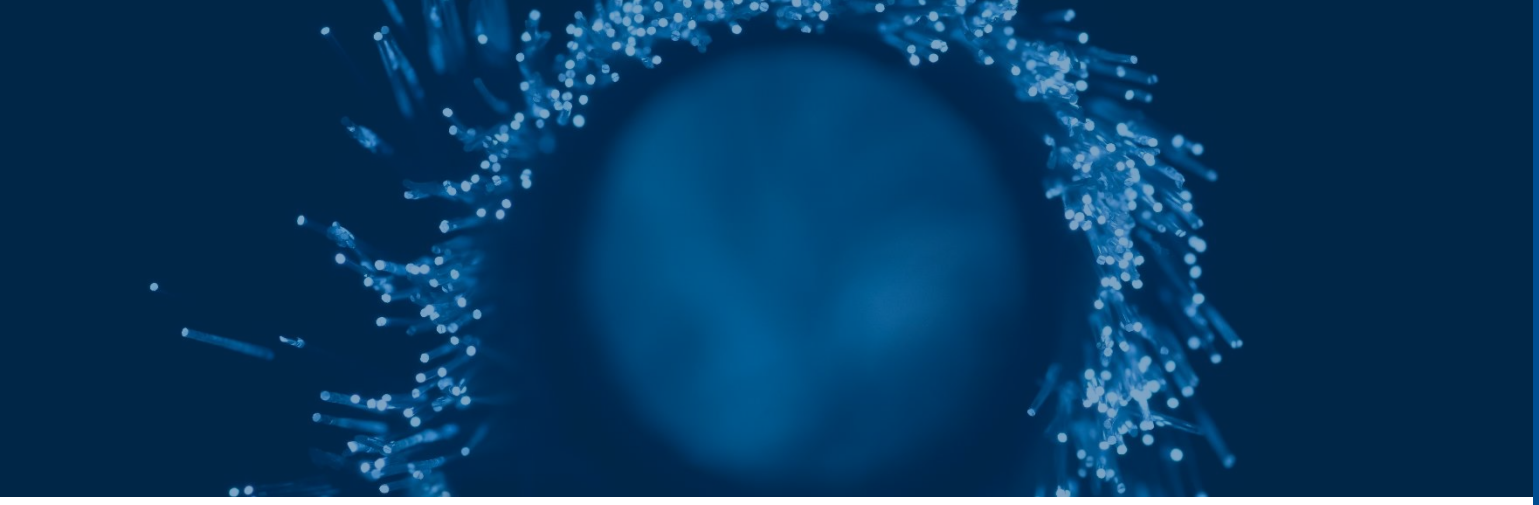


- Recent rulings by the Court of Justice of the European Union (CJEU) have further clarified the scope of data subjects' right of access (e.g. **C-154/21**, **C-487/21** and **C-579/21**). While these rulings provide much-needed **clarity**, they also represent a tightening of data protection requirements 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** for the fourth consecutive year. Although the sector cases differ, we would make an 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 data subjects' **willingness to bring (alleged) breaches of law to the attention of a DPA more quickly**. The same could apply to the employment sector, ranking second in the fines by sector table.

- Another trigger could be the **use of new technologies**, which is encouraged by the constant pressure to innovate in these industries. One such example is 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:

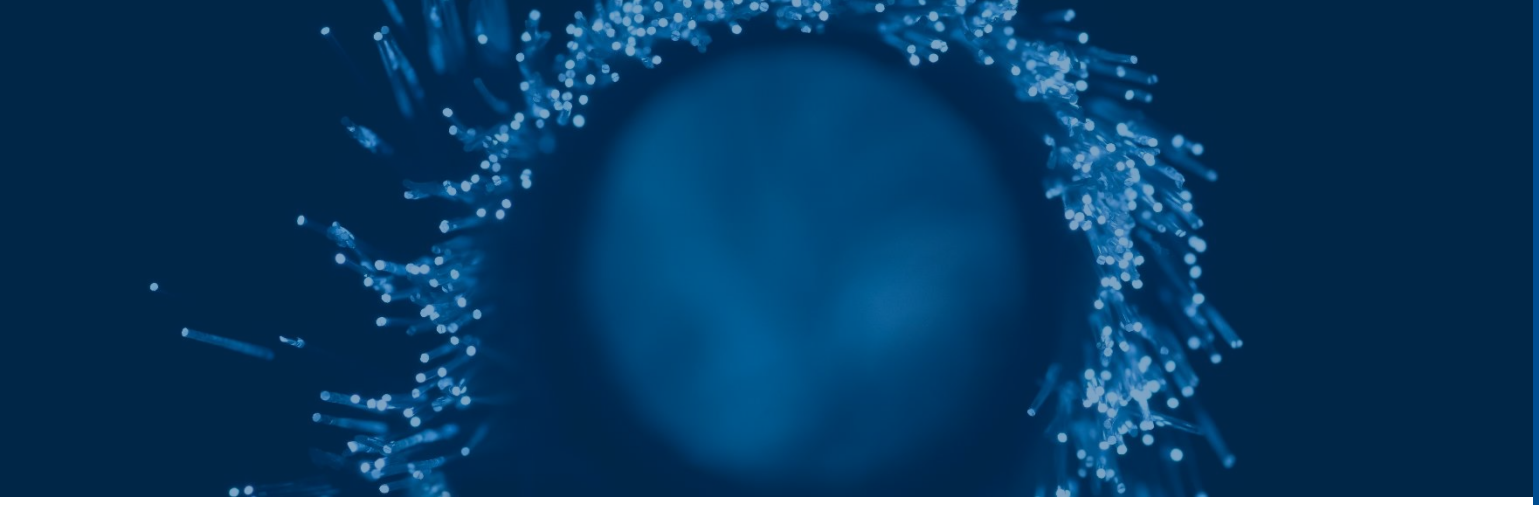
  "We will continue to monitor and assess new digital technologies to promote a human-centric approach, including those relating to, among others, Artificial Intelligence and digital identity. We will continue to issue guidance, where necessary, on the data protection implications of new technologies, 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.

- Seven years after the GDPR came into force, the European sanctions landscape has matured, but many questions 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 GDPR**.

- 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 CJEU 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. At the same time, civil rights organisations complain about enforcement deficits (even referring to a "**GDPR crisis point**"), especially against big tech companies, for precisely this reason.

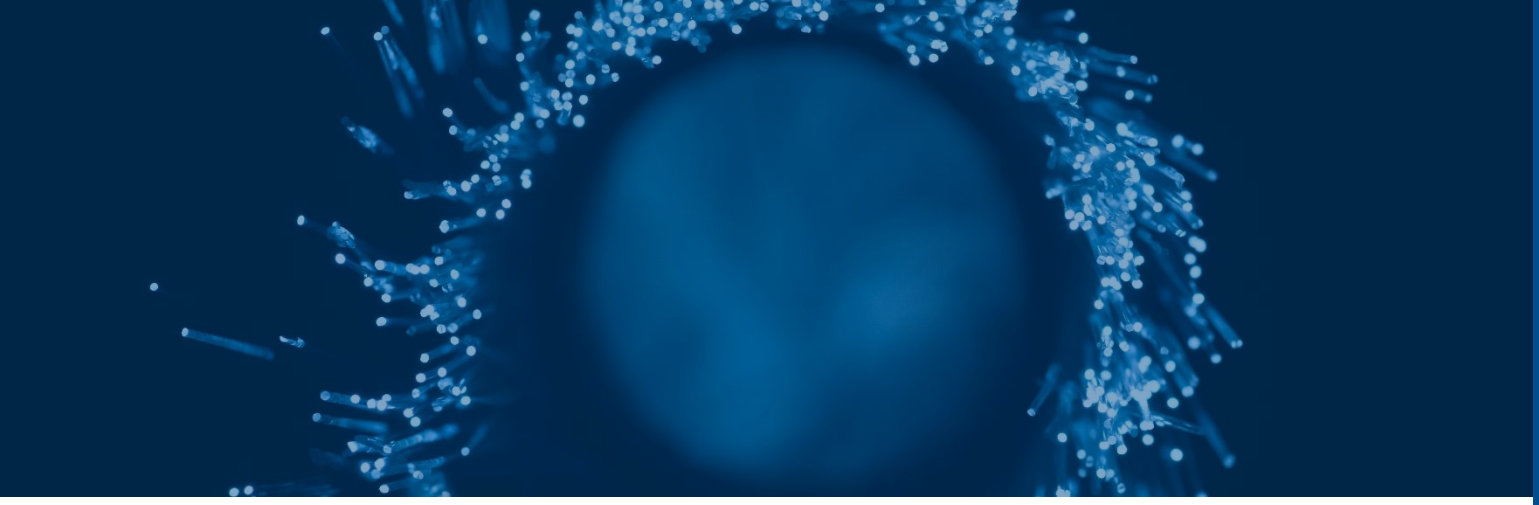
- This is exemplified by the recent practice of the Irish DPC, where significant fines, such as the record-breaking penalty against Meta of EUR 1.2 billion, were only imposed after a binding decision by the European Data Protection Board (EDPB).

- 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 by 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 compensation. 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 expect to be sued increasingly often by consumer associations for possible data protection violations.
- **In any case, GDPR enforcement will continue to keep privacy pros busy for another seven years – and most likely beyond…**

Enforcement Insights by Business Sector

Finance, Insurance and Consulting

The significant increase in the number of fines observed in the previous years in this sector continues. Furthermore, the amounts of imposed fines have significantly increased, with four fines exceeding EUR 1 million during the reference period of the 2025 ETR compared to two fines exceeding EUR 1 million during the reference period of the 2024 ETR.

The highest fines were all 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. Companies in the finance, insurance and consulting sector should implement comprehensive processes to ensure a clear legal basis for each data processing activity. The establishment of mechanisms to obtain effective consent from their customers where necessary is essential. DPAs seem to focus on how exactly consent was obtained and whether data subjects were fully informed by the controller.

Additionally, 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 becomes increasingly important. This sector is typically highly regulated and companies are subject to strict scrutiny regarding their data security and general IT security not only by DPAs but also by financial regulators.

Accommodation and Hospitality

In the accommodation and hospitality sector, data protection violations in the context of video surveillance remain the most important reason for the imposition of fines. Other important topics are cyber incidents that lead to data breaches or fraud incidents and the unlawful processing of ID cards.

At the same time, fines in this sector remain at a relatively low level, except where large hotel chains or online platforms are concerned.

Healthcare

There was only a moderate increase in the number of fines imposed compared to the previous year. The most common reason for fines in the healthcare sector continues to be the lack of sufficient technical and organisational measures (TOMs). This remained a common issue across many healthcare institutions and without a particular regional focus. In particular, the average fine for TOMs has increased significantly compared to the previous year, and a seven-figure fine has been imposed.

Industry and Commerce

In particular, non-compliance with general data protection principles and an insufficient legal basis for data processing resulted in severe fines for companies in the industry and commerce sector. Violations of the controller's information obligations towards data subjects were also closely investigated by DPAs. Especially the Spanish, Romanian and Italian DPAs continue to be very active and willing to investigate GDPR violations of all kinds. It is also notable that tech companies were subject to fines in this sector particularly regularly. The highest fine in this sector in 2024 was imposed against Clearview AI, which has become a "regular" for GDPR fines. The company had received previous fines from the DPAs in France, Germany, Greece, Italy and the UK, accumulating to more than EUR 100 million. This impressive amount is only topped by the two nine and eight-digit sanctions against the Amazon Group from previous years, which still make up more than 80 % of the total fine volume of the whole sector (EUR 778 million).

Real Estate

The real estate sector requires the processing of sensitive data, as prospective tenants provide landlords with information such as ID documents and detailed financial information, although landlords would be well advised to only collect data in the rental application process that are strictly necessary for the rental and to take the necessary measures to ensure security when processing personal data.

Furthermore, data controllers routinely collect and process data using CCTV systems to protect their property against theft, vandalism and other inconveniences. Adequate technical and organisational measures must be in place to ensure adherence to GDPR with a special focus on general processing principles such as data minimisation or storage limitation. Where a need for any kind of publication arises, caution should be paid to avoid unintentional disclosure of personal data, e.g., identifiable persons on pictures in advertisements.

Media, Telecoms and Broadcasting

The media, telecommunications and broadcasting sector is one of the most fined sectors. It makes up 70 % of the fines imposed on companies under the GDPR. Supervisory authorities are continuing to use the full frame of possible fines. Due to the big players in this sector and increasing relevance of personal data for their businesses, this sector will probably continue to be closely watched by supervisory authorities.

Many NGOs fighting for sufficient privacy have picked up on privacy issues and often tip off the authorities to start investigations. This trend might become even more relevant in the coming years since NGOs are now seeing the fruit of their work.

Transportation and Energy

While the number of fines in the transportation and energy sector has slightly decreased this year, the amounts of fines imposed by Data Protection Authorities have increased. The fines imposed by the Italian and Spanish DPA demonstrate a focus by these DPAs on abusive marketing practices and a failure by companies to take the necessary steps to stop unlawful activities. Consumer complaints to the DPAs partially initiated and impacted these investigations.

Where a larger number of consumers have been affected, the Spanish and Italian DPAs continue to impose hefty fines in the millions, while other countries' DPAs, with the exception of Finland and Greece, have not (at least publicly) imposed such fines for the transportation and energy sector in 2024.

Public Sector and Education

Public authorities hold a special position of trust that requires particularly strict compliance with data protection laws and an outstandingly high level of data security as they often process highly sensitive data and therefore are attractive targets for cyber-attacks and vulnerable to accidental disclosure. The same applies to schools and other educational establishments, in particular those that process personal data of minors. DPAs appear to have increased scrutiny of the public and education sector since the 2020 ETR, in particular in connection with the use of technology (e.g. online education tools used in schools and universities). It seems likely that this trend will continue in the future.

Further, the number of fines in the public sector for violations of data protection laws with regard to the processing of sensitive data in general as well as profiling and tracking or surveillance of individuals continues to grow. In this context, it is notable that the highest and the second highest fines in the public and education sector resulted from extensive and systematic collection and processing of personal data (including sensitive data) of citizens, mainly for statistical and profiling purposes.

.

Individuals and Private Associations

The number of fines and the total amounts for this sector have grown modestly since the 2024 ETR. Many small fines were imposed against individuals. More than 60 % of all fines in this sector were imposed by the Spanish DPA (219 of 360 cases).

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

For individual entrepreneurs and private individuals, the DPAs seem to have paid very close attention to the extent to which the violation was foreseeable by the individual and to the motives behind the processing. The number of data subjects and the infringing party's intention to pursue economic interests through the illegal data processing were particularly important.

Nearly half of all fines in this sector were based on illegal video surveillance. This underscores the general focus of DPAs on video surveillance. They consider video surveillance to be such a risky form of processing that strict requirements must be met even by private individuals.

Employment

We have noticed a significant increase in the total amounts of fines imposed to date, mainly due to the new ‘employment record fine’ in the amount of EUR 290 million imposed by the Dutch DPA 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. Moreover, employers increasingly rely on evidence based on the processing of personal data in employment court proceedings. In this context, employers are well advised to pay special attention when advanced technology is used for HR administration purposes: Automated decision making and/or processing of biometric data may appear tempting at first sight, but advanced technology comes with advanced obligations under data protection law, such as a requirement for data protection impact assessments.

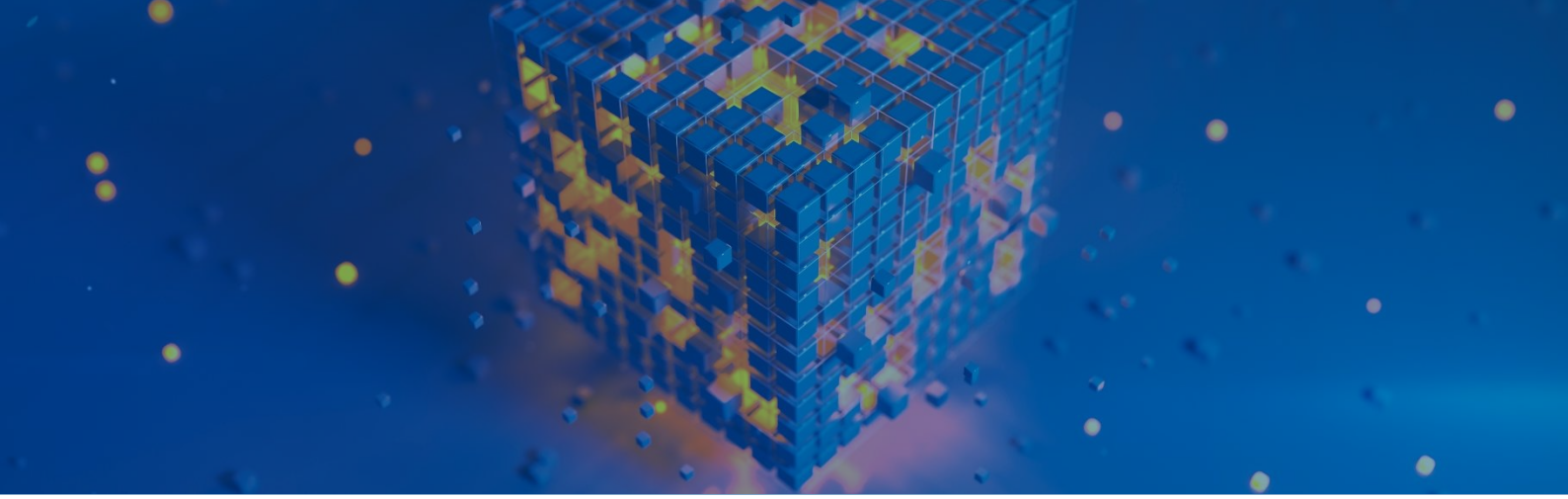
In addition, employees are more likely to request information on their stored data and – in case of conflict situations (including but not limited to cases ultimately brought to employment courts) – may resort to complaints to a DPA. Employees are increasingly exploiting employers' uncertainties about data protection to assert other legal positions against employers. It is worth noting that DPA inquiries frequently lead to additional findings beyond the scope of the original employee complaint.

In our experience, employers have had to justify their data protection compliance not only to DPAs but also to trade unions and works councils in recent years.

.

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. The established interpretation of such national employment laws usually influences the permit-ted extent of employee data processing.

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 seventh edition of the ET Report will be published in one year's time (around May 2026), 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 the absence of a global data protection law.

We have consulted with peers from the legal profession, privacy professionals with a more advanced tech background and researchers from various disciplines.

We strongly encourage you to continue with this interaction (info@enforcementtracker.com). We apologise in advance if it takes us some time to respond: the world of data protection has not calmed down and this process may go on for a while.

Enforcement Tracker Report 2025

Enforcement Tracker Report Key Editors

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

Michael Kamps
Partner
E michael.kamps@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, Dr Alexander Schmid

E info@enforcementtracker.com

CMS Data Protection Contacts

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

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

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
Ramón Valdivieso
E ramon.valdivieso@cms-ca.com

China
Jonathan Chu
E jonathan.chu@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

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

CMS Data Protection Contacts

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

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

Netherlands
Tom Jozak
E tom.jozak@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

João Leitão Figueiredo
E joao.figueiredo@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 Šímová
E martina.simova@cms-cmno.com

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

South Africa
Sihle Bulose
E sihle.bulose@cms-rm.com

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

Sweden
Jennie Nilson
E jennie.nilsson@cms-wistrand.com

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

Turkey
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