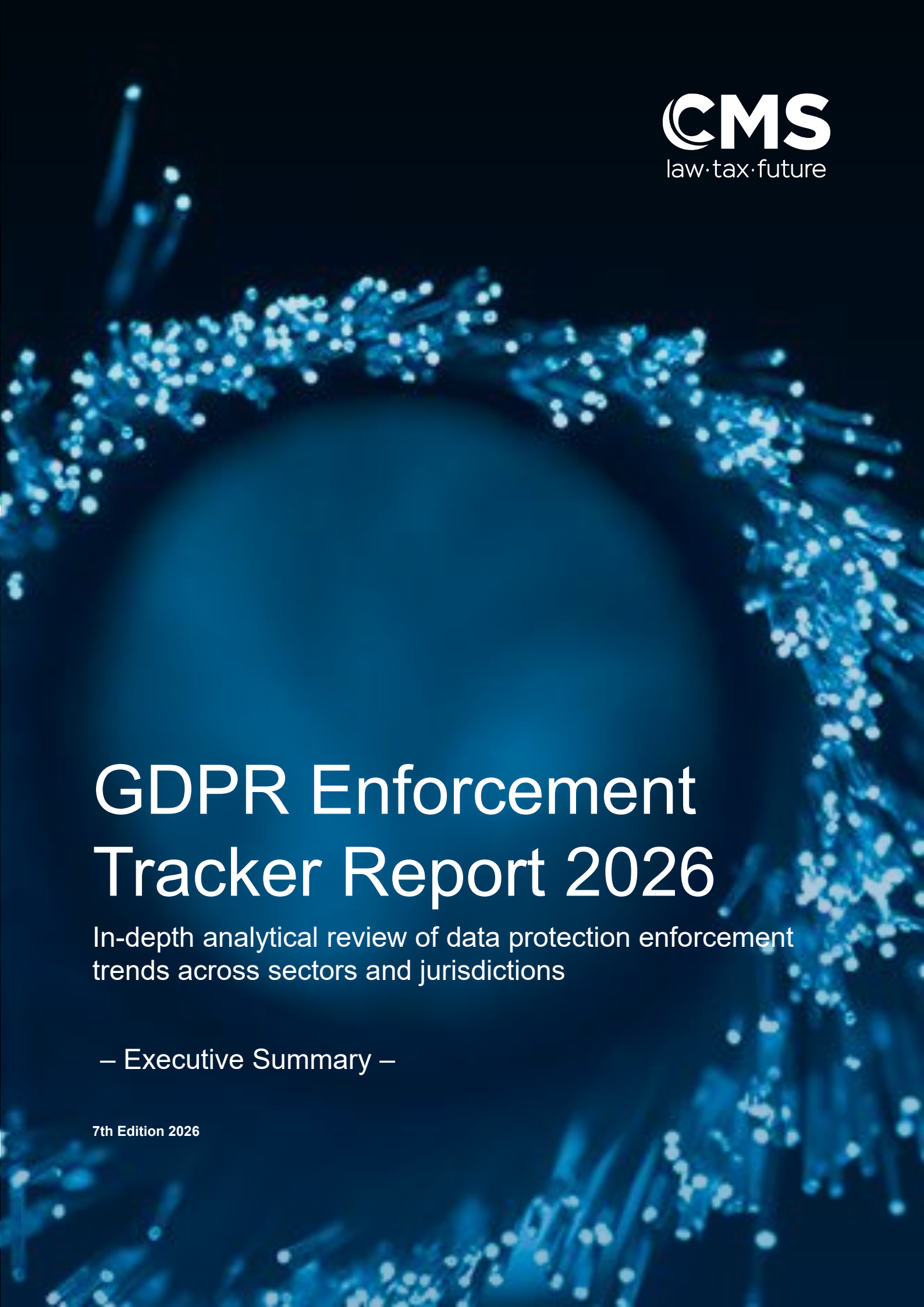


GDPR Enforcement Tracker Report 2026

In-depth analytical review of data protection enforcement trends across sectors and jurisdictions

– Executive Summary –

7th Edition 2026

Executive Summary – 2026

The CMS Data Protection Group is pleased to launch the 7th edition of the **GDPR Enforcement Tracker Report ("ET Report")** – CMS's annual flagship analysis of GDPR enforcement trends identified through the data captured by CMS's own **GDPR Enforcement Tracker**. This Executive Summary is our service for busy readers.

What the ET Report is all about

In the eight years since the General Data Protection Regulation (GDPR) became applicable, GDPR enforcement has significantly increased awareness of data protection compliance across sectors and jurisdictions. At the same time, GDPR enforcement has evolved considerably since 2018 and has become an established part of regulatory supervision across Europe.

We still believe that facts are better than fear.

The continuously updated **GDPR Enforcement Tracker** provides the factual foundation. Seven years ago, we expanded upon this approach by introducing the annual ET Report to provide a more in-depth analytical review of enforcement trends across sectors and jurisdictions. As in previous editions, the ET Report provides practical insights into the evolving enforcement landscape under the GDPR.

What is new in the ET Report's seventh edition?

This seventh edition of the ET Report covers all fines from 2018 to the editorial deadline of 1 March 2026. As of the editorial deadline, the Enforcement Tracker covered 3,062 fines (2,685 if only fines with complete information on the amount, date and controller are counted).

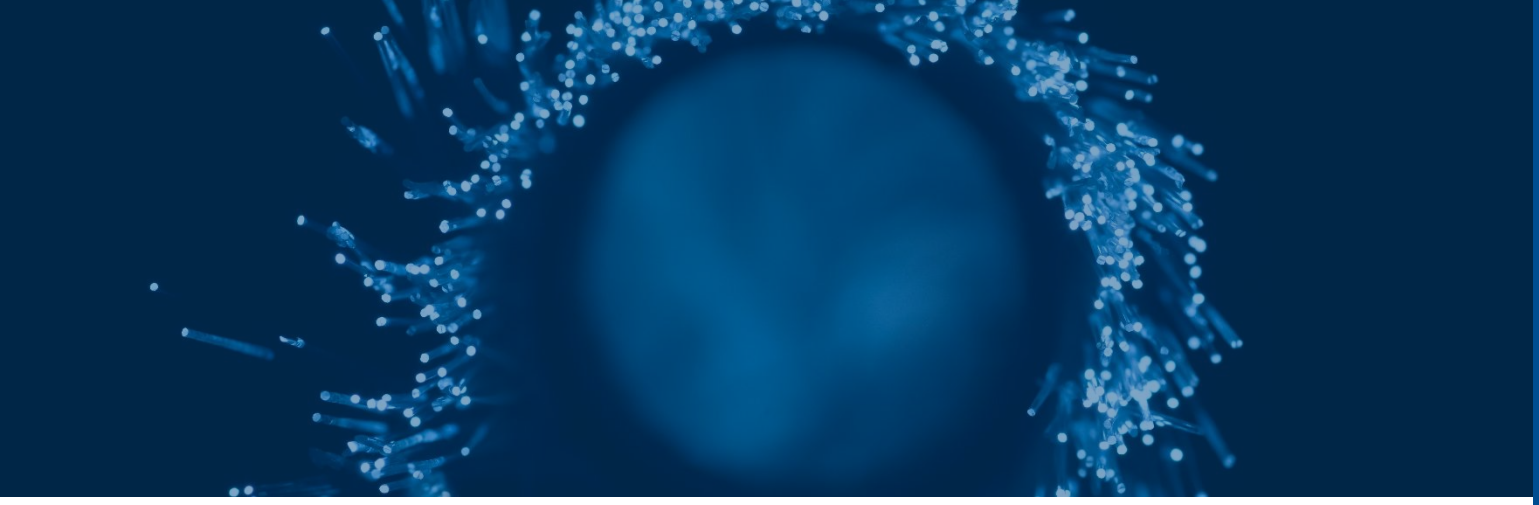
The ET Report opens with a "Numbers and figures" section summarising the record-ed fines, followed by "Enforcement insights by business sector" (including a dedicated employment section) and "Enforcement insights by country", providing additional context on national enforcement frameworks. This year's report reflects the continued shift towards more operational GDPR enforcement across Europe. In addition to large cross-border proceedings involving major technology companies, supervisory authorities are increasingly focusing on practical compliance topics such as transparency obligations, cybersecurity measures, online tracking activities, employee monitoring and emerging AI-related processing activities. In October 2025, the European Data Protection Board (EDPB) announced that the 2026 Coordinated Enforcement Framework (CEF) will focus on GDPR transparency and information obligations, underlining the growing relevance of enforcing these requirements across sectors and jurisdictions

Numbers and Figures

- As of March 2026, a total of 2,685 fines (+440 in comparison to the 2025 ET Report) were recorded in the Enforcement Tracker. The database also includes cases with limited or incomplete information, leading to an overall total of 3,062 recorded cases.
- Different approaches to the publication of fines and decisions are often root-ed in national law, as the publication of decisions may itself constitute a separate sanction in certain jurisdictions (see also the Enforcement insights by country). Nevertheless, European DPAs generally publish aggregated enforcement statistics at least annually, e.g. in their annual reports. Based on random sampling and publicly available enforcement statistics, the actual number of GDPR cases is likely to be significantly higher than what the Enforcement Tracker records.
- Total fines exceeded the EUR 6 billion mark for the first time, reaching ap-proximately EUR 6.11 billion (+487.6 million in comparison to the 2025 ET Report). Across the reporting period from 2018 to 2026, the average fine amounted to approximately EUR 2.28 million, although averages continue to be heavily influenced by a comparatively small number of exceptionally large fines.
- The highest GDPR fine to date remains the EUR 1.2 billion fine imposed by the Irish Data Protection Commission against Meta Platforms Ireland Limited in May 2023 due to unlawful international data transfers (ETid-1844). Following Luxembourg Administrative Court's decision to set aside the EUR 746 mil-lion Amazon fine and refer the matter back to the CNPD in March 2026, nine of the ten highest GDPR fines now originate from Ireland.
- "Insufficient legal basis for data processing" and "non-compliance with general data processing principles" remain the most frequent reasons for significant GDPR fines. "Insufficient technical and organisational measures to ensure information security" also remains a major enforcement trigger, particularly following cyber incidents and personal data breaches.

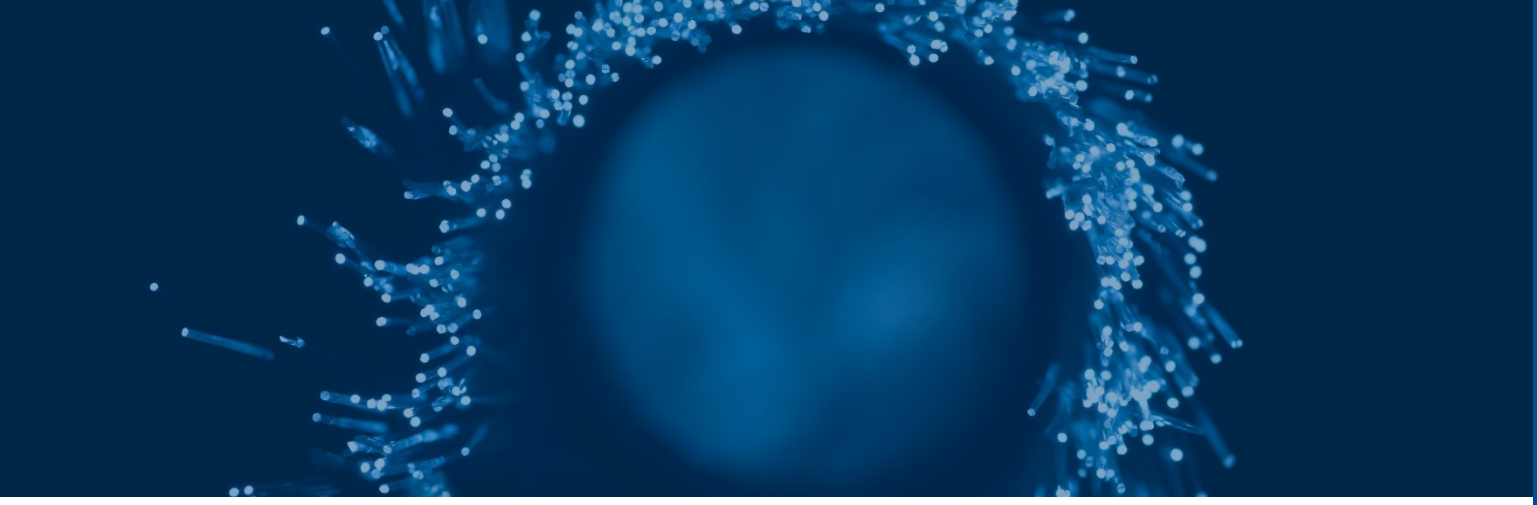
- Spain remains – for the seventh consecutive year – the jurisdiction with the highest number of published fines, again followed by Italy, Romania and Po-land. At the same time, the country reports show that publication practices, enforcement structures and fining philosophies still differ considerably be-tween Member States. The publicly available statistics therefore only partially reflect actual enforcement activity across Europe.

- The evolution of fines since 2018 illustrates the broader evolution of GDPR enforcement across Europe. While early enforcement focused primarily on establishing fining practices and landmark proceedings against major technology companies, supervisory authorities are now increasingly focusing on operational compliance issues across sectors, including transparency obligations, cybersecurity, online tracking, vendor governance and emerging AI-related processing activities.



Our overall takeaways

- Seven years after the GDPR became applicable, its enforcement across Eu-rope has clearly entered a mature stage. GDPR investigations and sanctions are now part of the routine supervisory practice of European authorities. At the same time, the country reports show that enforcement practices, procedural structures and fining cultures still differ significantly between Member States. Despite increasing coordination through the European Data Protection Board (EDPB), GDPR enforcement therefore remains only partially harmonised in practice.
- Transparency and user-facing information obligations are emerging as clear horizontal enforcement priorities across sectors and jurisdictions. Deficiencies relating to privacy notices, cookie banners, employee information and other transparency measures now regularly appear alongside unlawful processing and insufficient technical and organisational measures.
- Insufficient legal bases for processing, non-compliance with general data processing principles and insufficient technical and organisational measures remain the dominant GDPR fine triggers across Europe. Recent cases also show increasing regulatory scrutiny of vendor management, processor over-sight, Transfer Impact Assessments, Data Protection Impact Assessments, in-ternal access controls and accountability structures. Cyber incidents and data breaches are increasingly acting as catalysts for broader regulatory scrutiny, with supervisory authorities using such incidents to assess the overall adequacy of organisational security and accountability measures.
- Digital platforms, advertising-driven business models and large-scale consumer data ecosystems remain at the centre of GDPR enforcement. International data transfers, online tracking technologies, profiling activities and behavioural data processing continue to generate the highest fines. Supervisory authorities are also increasingly scrutinising AI-driven services, biometric technologies and facial recognition systems, particularly where vulnerable individuals or extensive profiling are involved.



- GDPR enforcement is increasingly extending beyond traditional commercial organisations. Supervisory authorities are increasingly applying GDPR standards to public authorities, sports associations, non-profit organisations and other membership-based structures processing significant amounts of personal data. Enforcement against private individuals also remains common, particularly in connection with unlawful video surveillance and misuse of access rights.

- Data subject complaints remain one of the most important practical drivers of GDPR enforcement. Employee complaints, access requests, direct marketing complaints and disputes regarding surveillance or transparency obligations frequently trigger investigations by supervisory authorities. Private enforcement through representative actions, NGO activity and collective redress structures continues to develop, although administrative enforcement by supervisory authorities still plays the dominant practical role in most jurisdictions.

- Judicial review is becoming increasingly important for the development of European data protection law. Large GDPR fines are regularly challenged before national courts and key questions regarding fining standards, procedural safeguards and substantive GDPR interpretation continue to be referred to the CJEU. While this trend may increase legal certainty over time, it also illustrates that important aspects of GDPR enforcement remain legally and procedurally contested across Europe.

Enforcement Insights by Business Sector

Finance, Insurance and Consulting

Enforcement in the finance, insurance and consulting sector continues to intensify. Digital onboarding, profiling, direct marketing and the use of customer data across financial and insurance services remain the primary focus of regulatory scrutiny.

The highest fines in this sector were primarily linked to insufficient legal bases for processing, insufficient transparency towards data subjects and failures in consent management. In several cases, controllers failed to demonstrate that customer consent had been validly obtained or was sufficiently granular for the relevant processing activities. DPAs closely scrutinise how customer data is collected, combined and used across online services and apps.

Deficiencies in technical and organisational safeguards continue to trigger significant fines, particularly where cyber incidents exposed large volumes of sensitive customer or financial data. DPAs are increasingly assessing data protection compliance, cybersecurity governance and outsourcing structures together rather than as isolated compliance issues.

Accommodation and Hospitality

In the accommodation and hospitality sector, unlawful video surveillance remains by far the most common trigger for GDPR enforcement. Many fines concern CCTV systems in hotels, restaurants and bars that do not comply with GDPR transparency and data minimisation requirements.

Cyber incidents and insufficient technical and organisational measures are becoming increasingly relevant, particularly where customer or payment data has been compromised. Supervisory authorities are also directing increased scrutiny at identity verification procedures and the processing of copies of passports or identity documents.

Overall, fines in this sector remain comparatively moderate. Most enforcement actions concern individual hotels, restaurants or smaller operators, while higher fines are typically associated with larger hotel groups, online booking platforms or large-scale customer databases.

Healthcare

DPAs have shown increasing willingness to impose substantial fines in the healthcare sector, including multi-million-euro penalties following cyber incidents and systemic deficiencies affecting the protection of sensitive health data.

Deficiencies in technical and organisational safeguards remain the dominant enforcement trigger. Supervisory authorities are focusing not only on ransomware attacks and external threats, but also on internal governance failures, including excessive access rights, insufficient role-based access controls, inappropriate software configurations and operational negligence.

DPAs continue to enforce general data processing principles strictly, particularly with regard to data minimisation and transparency obligations. Patient-facing privacy information and related documentation can be expected to receive increased regulatory attention under the EDPB's 2026 CEF.

Industry and Commerce

Insufficient legal bases for processing, unlawful tracking practices and breaches of general data processing principles continue to be the most common triggers for significant fines in the industry and commerce sector. Supervisory authorities continue to scrutinise transparency obligations and large-scale customer data processing.

The French CNIL fine against Infinite Styles Services Co. Limited (ETid-2864) illustrates the heightened enforcement risks for large online platforms deploying tracking technologies without valid consent. The scale of the platform, the volume of user data processed and deficiencies in cookie and transparency mechanisms were key factors underlying the EUR 150 million fine.

The enforcement actions against Capita plc and Capita Pension Solutions Limited (ETid-2898, ETid-2899) illustrate how cyberattacks increasingly trigger GDPR enforcement where underlying cybersecurity deficiencies become visible during incident investigations.

Although the EUR 746 million Amazon fine was set aside by Luxembourg Administrative Court in March 2026 and referred back to the CNPD, the case continues to illustrate the broader enforcement exposure associated with large-scale consumer data processing and digital platform business models.

Real Estate

Video surveillance, transparency obligations and the handling of tenant and property-owner data remain the dominant enforcement themes in the real estate sector. Although fines in the sector remain comparatively low overall, supervisory authorities continue to scrutinise CCTV systems, excessive data retention and unlawful disclosures of personal data.
Recurring compliance issues include overly intrusive camera placement, unlawful audio recording, insufficient information notices and the publication of personal data in semi-public settings such as residential notice boards or property marketing materials.

Direct marketing activities and excessive retention practices also generate enforcement risk. Several larger proceedings illustrate that supervisory authorities are willing to impose substantial fines where large-scale or systematic GDPR infringements are identified.

Media, Telecoms and Broadcasting

The media, telecoms and broadcasting sector continues to account for the highest overall GDPR fine volume, driven primarily by enforcement against large digital platforms and advertising-driven online business models.
Enforcement actions against TikTok, Google and Luka illustrate ongoing regulatory scrutiny of international data transfers, transparency obligations, online tracking and AI-driven services. In particular, supervisory authorities increasingly expect companies relying on Standard Contractual Clauses to conduct robust and well-documented Transfer Impact Assessments in light of Schrems II.
Transparency obligations are receiving increased regulatory attention. The EDPB's 2026 CEF further reinforces this trend.

AI-based and behavioural platform services involving vulnerable users or extensive profiling activities are likely to attract increased enforcement scrutiny, particularly where lawful basis, transparency or age verification mechanisms are insufficient.

Transportation and Energy

A relatively small number of high-value cases continue to shape enforcement in the transportation and energy sector, concentrated where large-scale infrastructure operators process personal data relating to millions of individuals.

Biometric identification systems, large-scale customer databases and extensive marketing practices involving external sales networks or intermediaries have drawn in-creased regulatory scrutiny. In particular, the Aena case illustrates the significant compliance risks associated with facial recognition technologies and insufficient Data Protection Impact Assessments.

Enforcement actions in the energy sector demonstrate that companies may face significant enforcement exposure where marketing partners or intermediaries process customer data unlawfully and adequate oversight mechanisms are lacking.

Public Sector and Education

The public and education sector remains a particularly active enforcement area, especially where authorities process sensitive personal data on a large scale or deploy technology-driven monitoring, profiling or identification systems.

Enforcement continues to focus on insufficient technical and organisational measures, large-scale data breaches and inadequate legal bases for processing. Several significant cases demonstrate increased scrutiny of biometric processing, surveillance-related technologies and extensive public-sector databases. Schools, universities and other public institutions remain under particular scrutiny where digital learning tools, remote monitoring technologies or large-scale student and citizen data processing are involved, especially where minors are affected.

Transparency obligations are becoming an increasingly important enforcement topic.

Individuals and Private Associations

Enforcement against individuals and private associations is characterised by a large number of comparatively small fines, with the Spanish DPA remaining particularly active.

Illegal video surveillance remains the dominant enforcement trigger. Supervisory authorities continue to treat CCTV systems as particularly intrusive processing activities, including where cameras are operated by private individuals in domestic or neighbourhood contexts.

Biometric technologies and facial recognition systems used by larger associations and sports organisations are attracting increased scrutiny. In several cases, supervisory authorities have imposed substantial fines for failures to conduct Data Protection Impact Assessments or to establish a sufficient legal basis for biometric processing.

Enforcement practice indicates ongoing regulatory scrutiny of misuse of access rights and unlawful access to internal databases, even where infringements involve individual actors rather than commercial organisations.

Employment

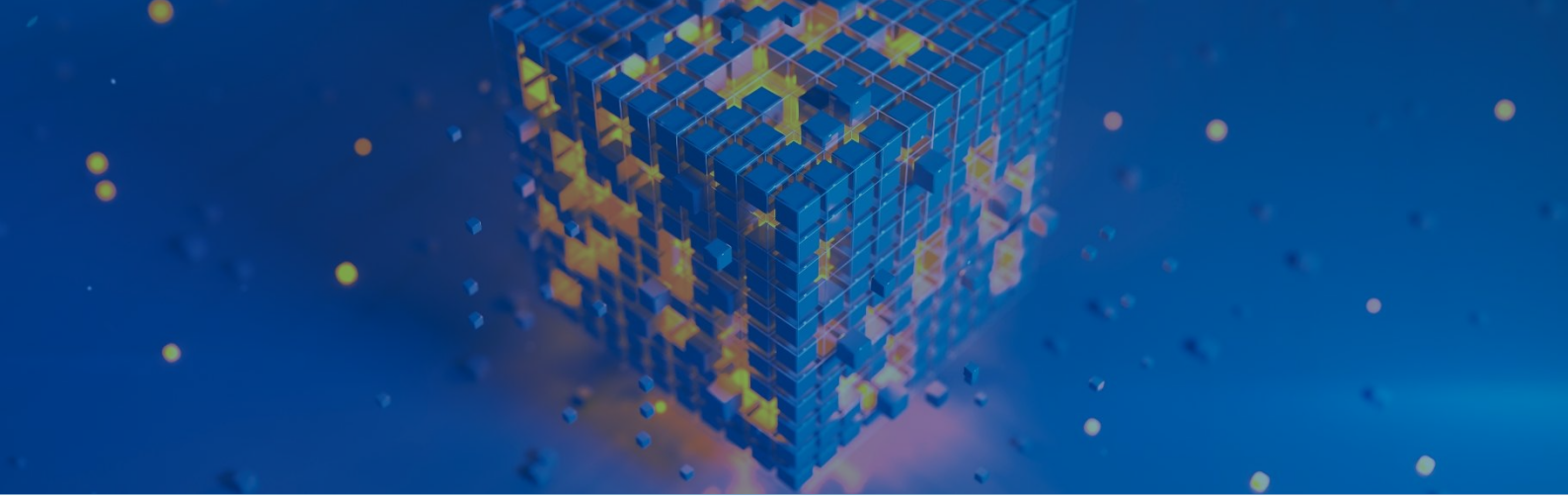
Employee data processing continues to be a core enforcement area under the GDPR, reflecting both the scale of employee-related processing across sectors and the increasing willingness of employees to trigger regulatory scrutiny through complaints and access requests.

International data transfers, insufficient processor oversight and employee surveillance practices are under increasing regulatory focus. The Dutch DPA's EUR 290 million fine concerning transfers of driver data to the United States and the Polish enforcement action against McDonald's Polska illustrate increasing scrutiny of vendor oversight, technical and organisational measures and cross-border HR processing structures.

Internal investigations, monitoring measures and employee transparency obligations are increasingly relevant enforcement topics.

Employment-related GDPR enforcement remains closely linked to national employment law frameworks, meaning that supervisory expectations and acceptable processing practices may continue to differ significantly between Member States.

.



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 eighth edition of the ET Report will be published in one year's time (around May 2027), 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 consultation with us (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 2026

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

Enforcement Tracker Core Team

Dr Alexander Schmid, Frederik Specht
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

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

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

China
Ulrike Glueck
E ulrike.glueck@cmslegal.cn

Colombia
Carlos Sanchez
E carlos.sanchez@cms-ra.com

Croatia
Karmen Sinožić
E karmen.sinozic@bmslegal.hr

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

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

Monaco
Stephan Pastor
E stephan.pastor@cms-pcm.com

CMS Data Protection Contacts

Montenegro
Milica Popović
E milica.popovic@cms-rrh.com

Netherlands
Tom Jozak
E tom.jozak@cms-dsb.com

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

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

Peru
Carolina Gajate
E carolina.gajate@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

Saudi Arabia
Ken Wong
E ken.wong@cms-cmno.com

Serbia
Dragana Bajić
E dragana.bajic@cms-rrh.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
Simone Brauchbar Birkhäuser
E simone.brauchbar@cms-vep.com

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

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

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

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