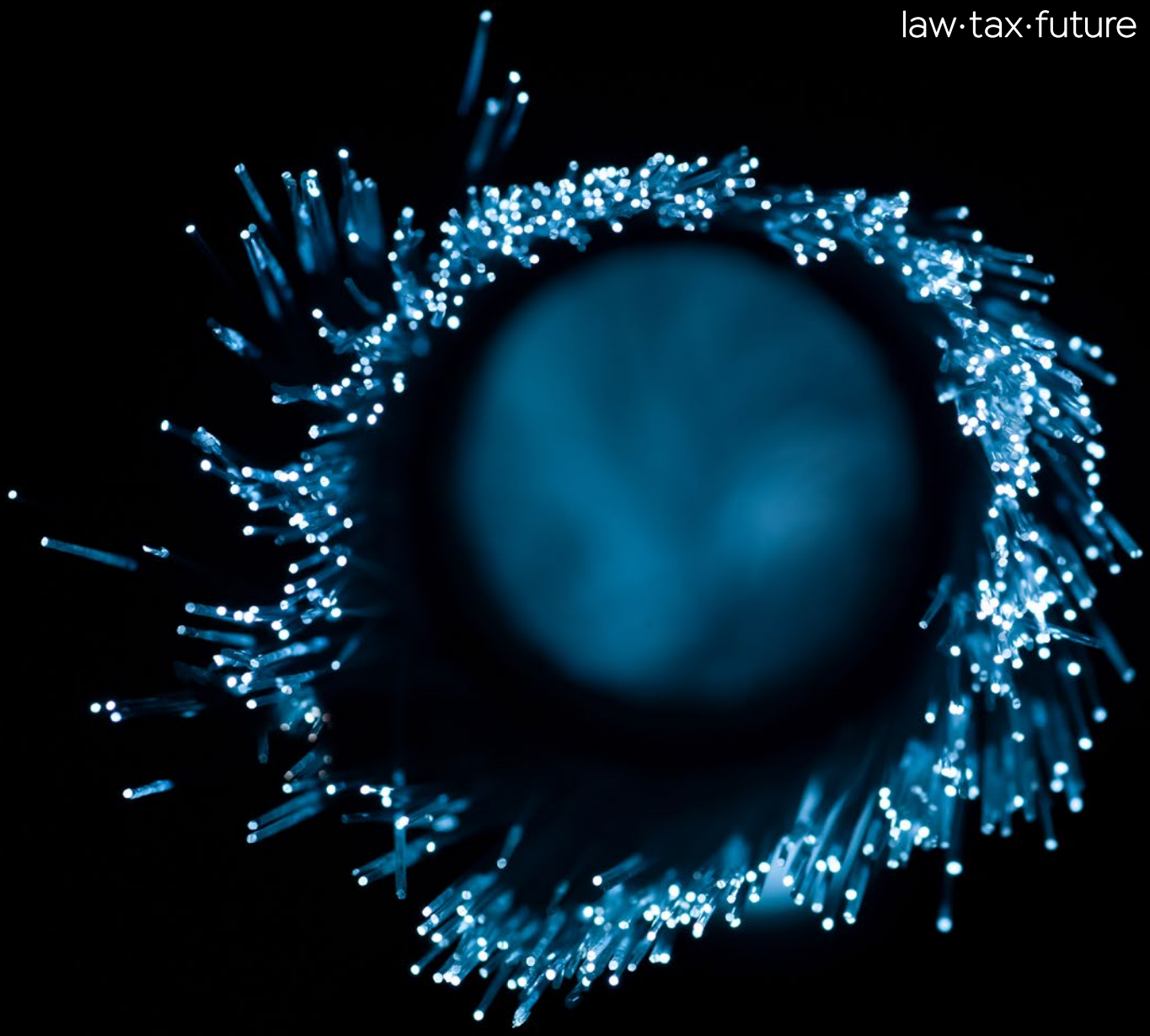
CMS
law·tax·future



GDPR Enforcement Tracker Report

Executive Summary

2nd Edition 2021

A warm welcome…

…to the second edition of the GDPR Enforcement Tracker Report ("ET Report"). This Executive Summary is our service for busy readers (somebody told us that privacy professionals have full schedules these days), also printable for bedtime reading without a digital device. The full ET Report is an online-only publication, available here.

What the ET Report is all about

When the GDPR was already in force, but not yet applicable (and not a single fine had been imposed yet), much attention was paid to the formidable fine framework. For many company officers, this caused fear: if I violate the GDPR, I have one foot in jail (or at least my organisation has to pay EUR 20 million or 4% of its global annual turnover, calculated for the whole group, if the company is part of one).

We believe that facts are better than fear.

Our continuously updated list of publicly known GDPR fines in the GDPR Enforcement Tracker is our 24/7 remedy against fear, while the annual ET Report is our deep dive and permits more insights into the world of GDPR fines. Please find some remarks on the Enforcement Tracker methodology at the very end of this Executive Summary.

What is new in the ET Report's second edition

The second edition of the ET Report covers all fines listed in the Enforcement Tracker between 25 May 2018 and the ET Report's editorial deadline of 1 March 2021. The second edition of the ET Report is therefore based on around 570 Enforcement Tracker entries (526 if only fines with complete information on the amount, date, controller and subject of the data protection violation are counted).

The ET Report contains an overall summary of the existing fines in the "Numbers and Figures" section and our overall takeaways, followed by a deep dive into business sectors as well as the overarching "Employment" category.

Numbers and figures

- The highest GDPR fine to date, of EUR 50 million, was imposed by the CNIL in France against Google, Inc in January 2019 due to an insufficient legal basis for data processing (ETid-23). The German H&M fine (ETid-405, approx. EUR 35 million, October 2020) and the Italian TIM fine (ETid-189, approx. EUR 27 million, January 2020) follow in the top three fine amount ranking.
- Spain – for the second consecutive year – leads the list of numbers of fines per country by a large margin, followed by Italy and Romania.
- The United Kingdom heads the list of average fines per country, followed by Germany and Sweden.
- Italy leads the list of total fine amounts per country, followed by France and Germany.


NEG7
BANKCALL
GOMARKF
FIXLOC
INTPRET
GETMKS
CDULOGIC
SCAXIS

- At the top of the list of types of violation both in relation to the number of fines and the average sum of fine are "insufficient legal basis for data processing" (202 fines, average EUR 820,000) and "insufficient technical and organisational measures to ensure information security" (114 fines, average EUR 560,000). These are followed by the catch-all category "non-compliance with general data processing principles" (Art. 5, GDPR – 86 fines, average EUR 220,000) and "insufficient fulfilment of data subjects' rights" (50 fines, average EUR 150,000).

Overall takeaways

- First high-level takeaway: **GDPR fines are not a temporary phenomenon but are here to stay**. European authorities (and yes, we are still including the UK in the Enforcement Tracker) issued fines totalling around EUR 260 million in 526 publicly known cases (where there is sufficient information to make it into our stats; there are more cases – see our methodology section).
- Another high-level takeaway: It may come as a surprise in view of the European legislator's intention to fully harmonise the regulatory framework through the GDPR, but **there is hardly an area that is (as yet) shaped more by national laws and official practice than GDPR fines**. The administrative/sanctions law environment as well as position, personnel and equipment, and finally an authority's self-confidence/understanding of its own role appear to vary significantly between EU member states. Truly understanding the variety of reasons for the "sanctions gap" in the EU will probably require more intensive and (different) professional research than our team of law firm privacy professionals can provide. For pan-European organisational risk management purposes, however, it should be noted that there appears to be a different factual risk level in relation to GDPR fines.

- **Insufficient legal basis for data processing** and **insufficient technical and organisational measures** top the "GDPR fine trigger" list. In addition, **non-compliance with general data processing principles** needs to be on the organisational risk management radar, as Art. 5 of the GDPR serves as a "catch-all provision" and covers almost all compliance requirements further specified in the other provisions of the GDPR. Corresponding fines may – in a nutshell – refer to almost any type of violation (we have already started a more detailed analysis of fines based on violations of Art. 5 of the GDPR vs. violations of more specific GDPR provisions).
- In line with a common factual GDPR risk assessment, data subject-facing cases of non-compliance also appear very likely to trigger fines. **Insufficient fulfilment of data subjects' rights and of information obligations** rank 4th and 5th in the type of violation list. What is sometimes perceived as an undue regulatory burden (i.e. defining and supervising appropriate processes to identify and deal with data subjects' (access) requests and ensure proper data processing information for relevant categories of data subjects) has to be taken seriously.
- **Sector exposure** is highest in **industry and commerce** and **media, telecoms and broadcasting** (the latter for the second consecutive year). The second sector may not come as a surprise as it includes digital media and platforms with a high likelihood of "risky" processing of consumer data. Factual risk is also triggered by data subjects being very aware of, and insisting on, their rights (as reflected in a larger number of complaints to and subsequent investigation by supervisory authorities).

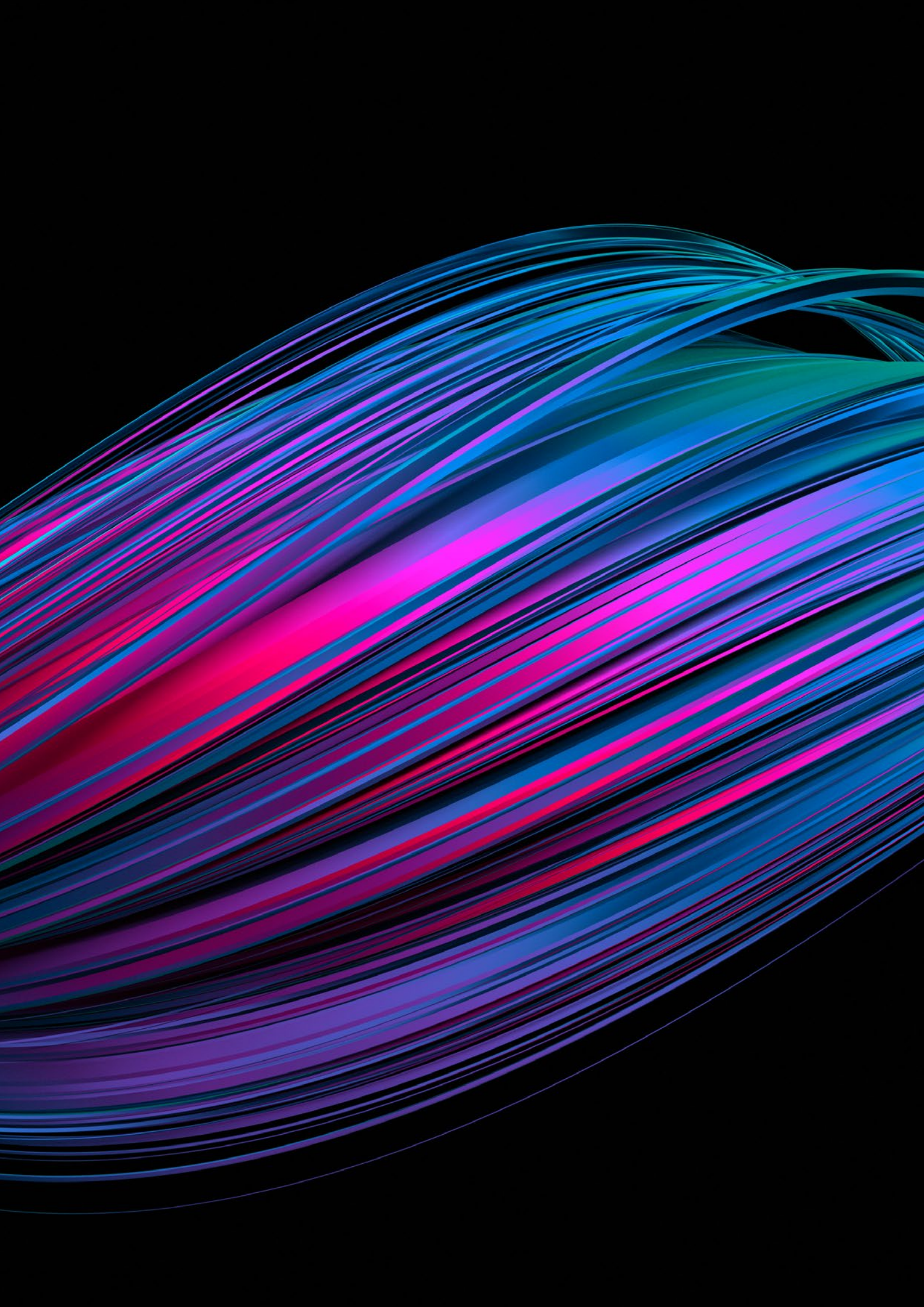
- Special attention should be paid to **video surveillance (CCTV) measures**: Regardless of the initial impression that CCTV is a common phenomenon in a variety of EU member states, it always was and remains a specifically intrusive measure from a "rights and freedoms of data subjects" perspective. The regulatory framework for CCTV also illustrates that **appropriate risk management requires a deep dive into the details** (and corresponding documentation). Non-compliance is rarely caused by CCTV operation as such, but by unnecessary excess in terms of detailed implementation (e.g. number/angle of cameras, areas of surveillance or retention periods) or by a lack of transparency (e.g. no CCTV signage/information for data subjects). Organisations are, therefore, well advised to **perform an extensive factual, legal and technical assessment before designing and installing CCTV** (and as always in data protection law, the definition of purposes is the starting point of everything). The good news is that CCTV can be operated in a compliant manner; the bad news is that an approach that works in one situation or one member state may not be fit or compliant in another situation or another member state.
- We also noted a significant number of GDPR fines due to **unsolicited direct marketing** (a risk frequently triggered by intrusive means of communication such as phone or email). Here again, regulatory details (with **possible distinctions between B2B and B2C** direct marketing) may vary between member states. And one message obtained from marketing/brand reputation specialists rather than from the legal department turns out to be true: be wary if you (despite your professional role) would not be happy to be approached in a certain way as a private person. Immanuel Kant's categorical imperative (or – less academically – decent common sense) may be important as overall guidance in data protection law as well.
- "It ain't over till the fat lady sings" – we are aware of the colloquial character of this phrase, but the essence turned out to be true in relation to GDPR fines. Unlike one year ago, we have seen a variety of (high profile) cases where **fines were significantly reduced during administrative procedures or after a supervisory authority's decision was challenged in court. These cases include** the "record fine cases" of the ICO against British Airways (ETid-58) and Mariott (ETid-60) – both reduced by the ICO compared to the initial notice, as well as one of the major German cases, Deutsche Wohnen (ETid-98 & ETid-99 – reduced by the competent court of first instance). You may wish to jump to the Member State Interview 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.

Takeaways per sector

Finance, Insurance and Consulting

Fines in the finance, insurance and consulting sector have increased significantly over the past 12 months, with several fines now ranging in the millions. Strikingly, the highest three 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 processing the data.

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 the 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 be looking 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 may 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.

Data security will become even more important as more and more financial and insurance services are performed digitally, e.g. via online banking, payment apps or insurance apps, or rely on cloud infrastructure. This applies all the more since 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

In the future, even small companies in the hospitality sector – including the kebab stand next door – should be careful not to be too eager to collect their customers' data. In particular, the strict requirements for permissible use of video surveillance/CCTV should be carefully examined in each individual case to avoid fines. Ill-judged surveillance of customers can quickly result in a fine. Data protection authorities have long since ceased to focus solely on the big players in the industry.

In terms of numbers, however, the risk of fines for inadequate security measures is much higher. There may be a trend emerging here, showing that negligence in providing for adequate technical and organisational measures is sanctioned with particular severity.

Health Care

The key issues regarding data protection in the health care sector concern technical aspects of data protection and, in particular, inappropriate setup (or lack thereof) of access management systems. Especially in hospitals, IT systems for processing patient data frequently appear to be open to the entire workforce without sufficient restrictions.

The reasons can only be inferred, but may be due to the fear that access restrictions and usability issues (such as forgotten passwords or lost security tokens) may obstruct fast access to the relevant patient data to the detriment of patients.

This seems to be a common issue across many health care institutions and does not have a particular regional focus, thereby indicating a general issue. This could be an occasion for all stakeholders involved – such as health care institutions, software developers and data protection authorities – to join forces to develop access protection systems that meet both the need of the health care professionals to have unobstructed and expedient data access and also data protection requirements.

Industry and Commerce

The industry and commerce sector experienced severe fines for non-compliance with general data protection principles and insufficient data security measures. DPAs have shown that they are willing to impose 6 or even 7-figure fines for insufficient TOMs, especially when large amounts of personal data are exposed to the public. The example of Carrefour France (ETid-457) shows that smaller violations can be sanctioned individually and add up to large overall fines.

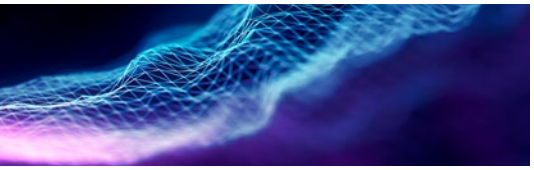
Real Estate

In the real estate sector, special attention must be paid to general processing principles when collecting and processing tenant data or using technical measures to protect buildings and assets against damage to property, theft or other detrimental effects.

The exceptional fine against Deutsche Wohnen SE is currently suspended, but it remains to be seen how the case will proceed following the public prosecutor's appeal.

Media, Telecoms and Broadcasting

DPAs have mostly levied fines in the media, telecoms and broadcasting sector because companies processed personal data without sufficient legal basis. In particular, DPAs in Italy and Spain have recently underlined that they are tackling telecom providers' unsolicited marketing communications as an unlawful part of their wooing of customers. Companies in the media, telecoms and broadcasting sector must typically obtain data subjects' consent prior to communicating marketing materials by phone or email. In addition, when obtaining data subjects' consent, companies must be particularly cautious and transparent: declarations of consent are only valid if they are freely given, specific, informed and unambiguous.



Apart from processing without sufficient legal basis, DPAs are still imposing numerous fines because companies fail to implement sufficient data security measures. Standard measures must include physical and system access controls, data pseudonymisation, availability controls and measures to ensure quick data restorability. All security measures must also be reviewed on a regular basis and tailored to the specific data processing scenarios. In particular, media and telecoms companies' large-scale processing operations require robust safety measures to bolster data subjects' data confidentiality and integrity.

Transportation and Energy

The fines imposed in the transportation and energy sector illustrate – as in other sectors – that companies must ensure sufficient technical and organisational measures (TOMs) and thus data security, especially when it comes to processing high volumes of customer data and/or sensitive information. Even though most of the fines imposed for insufficient technical and organisational measures did not exceed EUR 10,000, the British Airways example shows that large-scale violations may trigger an enormous risk of extremely large fines. There must also be an appropriate legal basis for any data processing. Here, the prerequisites of consent under the GDPR and national data protection law must be observed. Otherwise, there is a risk of heavy fines, particularly but not exclusively in the UK and Spain, with Spain being accountable for all fines imposed due to an insufficient legal basis in this sector in 2020.

As expected, the severe impact of the Covid-19 crisis on parts of the transportation (and energy) sector also (partly) affected – or rather reduced – the fines in this sector. This trend will most likely continue, at least with regard to companies that have been hit hard by the crisis. This is not only due to possible leniency in the context of the Covid-19 crisis on the part of the DPAs, but mostly down to the fact that the amount of the fine is calculated as a percentage of total worldwide annual turnover for the preceding financial year, which will be drastically lower for many companies in this sector.

Public Sector and Education

Public authorities have a special position of trust that requires particularly strict compliance with data protection laws and an outstandingly high level of data security. The same applies to schools and other educational estab-lishments that process personal data of minors. DPAs appear to have stepped up their scrutiny of the public and education sector since the ET Report 2020, in particular in connection with the use of technology during the Covid-19 pandemic. We consider it likely that this trend will continue in the coming years. In 2021, topics such as digital vaccination cards and coronavirus tracing are already and will continue to be of particular relevance.

Individuals and Private Associations

The total value of fines imposed against individuals and private associations remains almost identical compared to the ET Report 2020. Most fines were imposed by the Spanish authority. Many cases involve video surveillance on private grounds or in traffic (dash cams).

In this sector, the DPAs seem to take very close account of the extent to which the violation was foreseeable by the individual and of the motives behind the processing. The number of data subjects and the violator's intention to pursue economic interests through the illegal data processing was particularly important. At the same time, the intimacy of the processed data was also of considerable significance for the fine.

As is the case with companies, individuals and private associations primarily have to ensure that they can rely on a sufficient legal basis for processing operations and that they observe the data processing principles specified in Art. 5 of the GDPR.

Employment

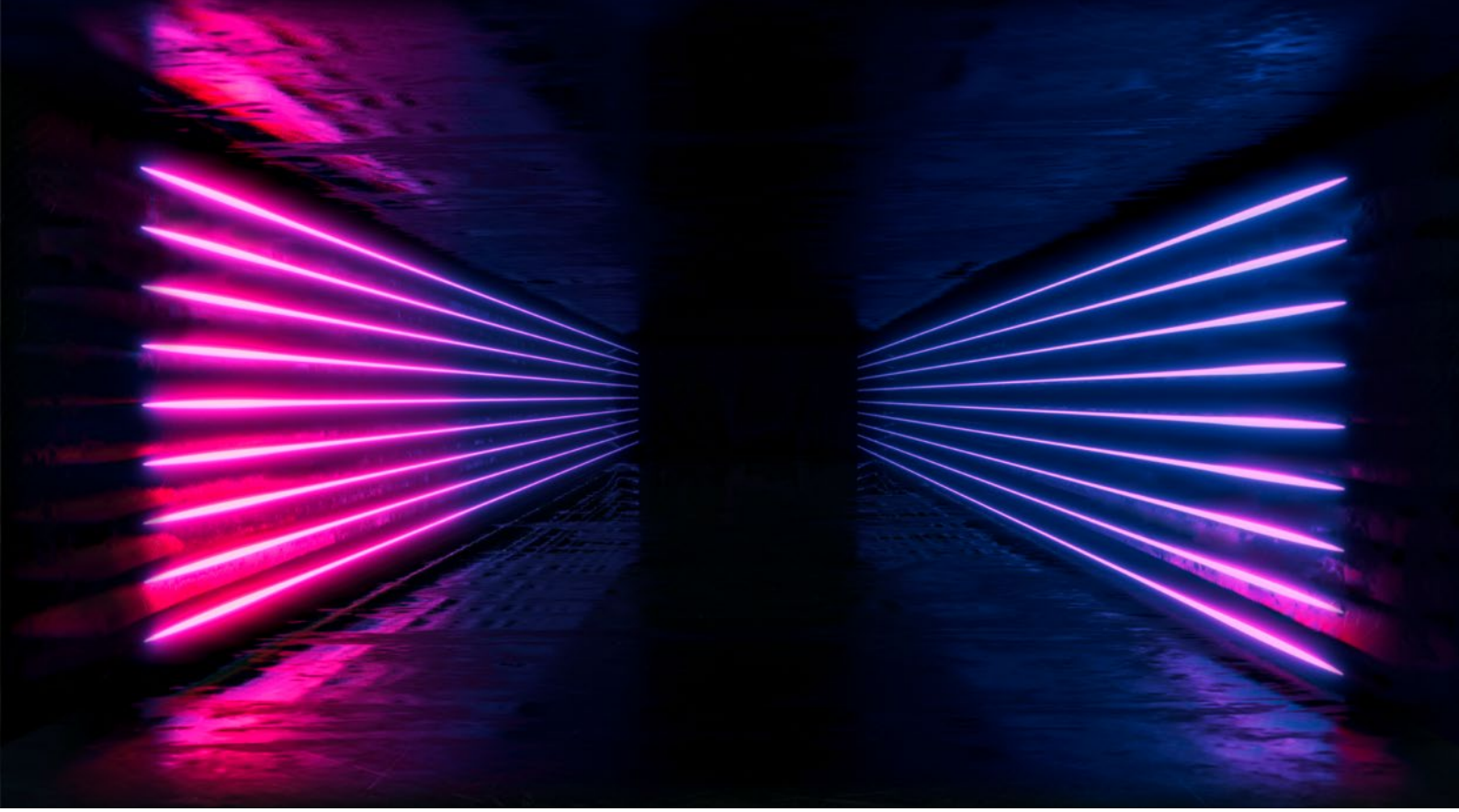
We expect the protection of employee data to become an established and key field of activity for DPAs, considering the overall importance of pro-cessing such data for companies of any size and in all sectors. Moreover, employers increasingly rely on evidence based on the processing of personal data in employment court proceedings.

In our experience, employers have had to justify their data protection com-pliance not only to DPAs but also to trade unions and/or works councils in recent years. Employees are increasingly exploiting employers' uncertainty about data protection to assert other legal rights against employers.

At the same time, cases involving the processing of employee data remain legally complex. 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 permitted extent of employee data processing.

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 working in the Enforcement Tracker engine room and preparing the Enforcement Tracker 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 work in progress. While the third edition of the ET Report will be published in one year's time (around May 2022), we highly appreciate any form of feedback (preferably constructive…) and would like to thank everybody who has reached out to us so far.

We have received many interesting ideas, information about forgotten or hidden fines and recommendations for additional features (our bucket list is growing steadily), as well as relevant contributions from stakeholders outside the EU – demonstrating that the data protection landscape is evolving rapidly on a global scale and interfaces between national/regional concepts are developing even in the absence of a global data protection law. We have engaged 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 keep this conversation going. And we apologise in advance if our feedback may take some time; the data protection world is not a quiet one right now...

Contact

Christian Runte
Partner
CMS Germany
T +49 89 23807 163
E christian.runte@cms-hs.com

Michael Kamps
Partner
CMS Germany
T +49 221 7716 372
E michael.kamps@cms-hs.com