A warm welcome…

…to the third edition of the GDPR Enforcement Tracker Report (“ET Report”). This Executive Summary is our service for busy readers (somebody told us that privacy professionals’ schedules are overflowing almost constantly since 2018), 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

Three years after the applicability of the General Data Protection Regulation (GDPR), its powerful fine framework still seems to be the focus of public attention (just as the European legislator intended). The threat of fines of up to €20 million, or 4% of an organisation’s annual global turnover, has certainly raised awareness and contributed to compliance efforts. Nevertheless, severe threats can also lead to fear and reluctance or ignorance on compliance issues.

We still 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. We started to extend our offering to the annual ET Report as deep dive approach three years ago. As in the previous two 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 third edition

The third 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 2022. The third edition is therefore based on around 1,088 Enforcement Tracker entries (1,031 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 our “Enforcement Insights” for various business sectors as well as for the overarching employment category.
What a year

2021 was an interesting year for a view on GDPR enforcement for several reasons.

For the first time since May 2018, the total number of cases recorded in the Enforcement Tracker exceeded one thousand. We think that this critical mass is an even better basis for our search for trends and patterns.

At the same time, the total sum of one billion euros in GDPR fines was exceeded for the first time in the summer of 2021, also driven by several record fines imposed on well-known digital stakeholders between March 2021 and March 2022. The record amounts of these landmark cases still have a significant impact on the statistics and attracted attention beyond the data protection bubble.

Finally, just as we were putting the finishing touches to this Executive Summary, the European Data Protection Board published its new “Guidelines on the calculation of fines” (initially for consultation), ensuring that the topic of “GDPR enforcement” will continue to occupy us.

Numbers and Figures

- Up to March 2022, a total number of 1,031 fines (+505 in comparison to the 2021 ET Report) were issued and recorded in the Enforcement Tracker (the database also includes cases with limited / no detail information, leading to an overall total of 1,088 cases).

- The total sum of fines amounts to around EUR 1.581 billion (+1.319 billion in comparison to the 2021 ET Report). In the reporting period 2018-2022, the average fine was around EUR 1,533,910 across all countries. The increase in total and average figures is mainly due to some massive 2021 fines against “Big Tech”.

- The highest GDPR fine to date in an amount 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). An Irish fine (approx. EUR 225 million, September 2021, ETid-820) and a French case (approx. EUR 90 million, December 2021, ETid-978) follow in — and have significantly changed — the top three fine ranking.
Leading the top list of types of violation both in relation to number of fines and average sum of fines are “insufficient legal basis for data processing” (342 fines, average EUR 1.2 million) and the “umbrella’ category "non-compliance with general data processing principles” (Art. 5 GDPR, 223 fines, average EUR 3.5 million). Next ranks go to “insufficient technical and organisational measures to ensure information security” (198 fines, average EUR 400,000) and “insufficient fulfilment of data subject’s rights” (95 fines, average EUR 180,000).

Spain is – for the third 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 of average fine amounts as well as of total sum of fines per country, again reflecting the impact of the dominating big tech record fines imposed in 2021.

The GDPR enforcement iceberg (and our high-level takeaways)

Reaching the critical mass of more than 1,000 cases and a total fine amount of more than one billion euros has also shaped the perspective of our analysis team.

The GDPR fines remind us of an iceberg: at the top and widely visible are the record fines / landmark cases – those in our top 10 list, for example. Below them – only visible with a closer look – are the other publicly known cases, i.e. those listed in the Enforcement Tracker. As with the 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 made public otherwise.

While we are still working to shed more light on the invisible cases (more on this likely in next year’s edition of the ET Report), 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 exactly is the accusation of having violated applicable law? Looking into the details of the cases often shows that controllers do not per se carry out unlawful data processing – frequently the unlawful scope of an otherwise permissible data processing is sanctioned.

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

- **We already stressed this aspect in last year’s ET Report, but it proves true the longer the more:** There is hardly an area of European data protection law (still) shaped more by national laws and official practice than the GDPR fines. The administrative / sanctions law environment as well as an authority’s position, personnel and equipment, and finally its self-confidence / understanding of its own role appear to vary significantly between European countries – anything but fully harmonised. Truly understanding the variety of reasons for the “sanction’s gap” will still require more intensive and (different) professional research than our team of law firm privacy professionals can provide. As a starter, we have, however, collected some Enforcement Insights per country (available in the ET Report from end of June 2022).

- **Regardless of enforcement variations across countries, GDPR fines continue to be serious and are here to stay.** Record fines / landmark cases should not obscure the constant increase in the total number of all cases – DPAs have operationalised fine procedures despite certain remaining legal uncertainties and variations in the application of the law.

- **Insufficient legal basis for data processing and insufficient technical and organisational measures** as well as **non-compliance with general data processing principles** are leading the “GDPR fine trigger” list and need to be on the organisational risk management radar. However, especially the “catch-all provision” on general data protection principles in Article 5 GDPR may be difficult to grab, 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 in absence of an official priority of GDPR compliance requirements, 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 type of violation list. Considering the complexity of dealing with, e.g., data subject’s 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.
• **Sector exposure** is highest in **industry and commerce** and **media, telecoms and broadcasting** 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 a reference to the **risks of monitoring persons**, which is already familiar to our loyal readers. Although the focus of these cases is still on **video surveillance (CCTV)**, the criteria visible there for the use of invasive means of surveillance could also be **relevant for other technical innovations**. The more risks an innovative technology may pose for the “rights and freedoms of data subjects”, the more **appropriate risk management requires a deep dive into the details** (and corresponding documentation). For this purposes, it is necessary to **perform extensive factual, legal and technical assessment before designing and installing innovative technology**. And as always in data protection law: the definition of purposes is the starting point of everything.

• 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 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.
The increase of fines in the finance, insurance and consulting sector (already observed over the last years) has continued, with additional fines ranging in the millions. Strikingly, the highest four 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.

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 applies all the more 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 recent cases indicate that especially non-compliance with general data protection principles may result in fines even for SME. On a larger scale, DPAs have shown that they are willing to impose 5-, 6- or even 7-figure fines, especially when large amounts of personal data are exposed due to insufficient data security measures (blending into a cross-sector trend and emphasising the importance of data security).

Healthcare

The key causes of fines in the healthcare sector continue to originate from technical and organisational data protection deficiencies and in particular inappropriate setup (or lack of) access restrictions and access management systems. This remained a common issue across many healthcare institutions and without a particular regional focus. However, it is noteworthy that in the past year, the authorities in Sweden and Italy have been particularly active in the field of healthcare.

In addition to technical and organisational measures for prevention of data breaches, it is advisable to also implement measures helping to identify the start, duration and scope of a potential attack in order to be able to adequately inform the authorities and affected data subjects. Lack of such measures for managing the worst-case scenario became subject to a fine in the past year.

The COVID-19 pandemic showed that the existing digital data processing structures were not yet ready to meet newly arising needs. New systems had to be set up rather quickly which led to the use of readily available, but inappropriate tools and lack of further organisational measures.
Industry and commerce

The industry and commerce sector experienced severe 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 storage periods. With some record fine cases in the industry and commerce sector, special attention will be paid to any appeal against / judicial review of DPA fining decisions.

Real estate

Businesses in the Real Estate sector frequently perform “high risk” processing activities – ranging from processing prospective tenant’s ID documents or detailed financial information to the operation of CCTV systems (often by data processors/service providers) to protect property against theft, vandalism and similar inconveniences. The implementation of adequate technical and organisational measures is key, as is a special focus on general processing principles such as data minimisation or storage limitation.

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. The French CNIL has prominently fined Google and Facebook for their unlawful cookie management / consent management systems. The cases are precedents for all operators of websites, apps and comparable digital offerings with “links” to end user devices. Compliant setups must facilitate an easy choice for users, including the rejection of cookies. The significant fine against WhatsApp also illustrates the importance of compliance with the transparency principle. Companies must provide an easily accessible and intelligible privacy policies for all relevant data processing operations, including for intra-group transfers of personal data. In doing so, the transparency principle can be utilised to foster customers and users trust.
Transportation and energy

As an exception to the overall trend of increasing fine numbers, the cases in the transportation and energy sector have decreased compared to recent years. On the other hand, the average fine amount has increased. The latter could be explained by some sort of less cautious attitude of the DPAs, especially in member states where the economic impact of the COVID-19 crisis has turned out to be less severe than initially expected.

Despite fines in the transportation and energy sector being the highest across all sectors by far, they are still comprised of the same criteria: In particular, the amount of data subjects involved and the severity of the single violations, but also the willingness to cooperate with the respective DPA have represented important factors in determining the amount of the fines.

Several DPAs have imposed fines in the transportation and energy sector for the first time since the GDPR came into effect. Some DPAs, in particular the Italian Garante and the Spanish AEPD significantly increased their fines. The majority of DPAs focused specifically on the legal basis and the purposes of the data processing. However, the number of fines for lack of technical and organisational measures was substantially lower in this sector. It could be that the sector has responded well to the close monitoring of this issue by DPAs in recent years.

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 establishments, 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 during the Covid-19 pandemic. In 2021, the majority of fines in the public sector have been imposed on educational institutions. Depending on the future impact of COVID-19 management, more related violations may be sanctioned in the coming years. Further, the number of fines in the public sector for violations of data protection law with regard to the processing of sensitive data (e.g. health data), profiling and tracking or surveillance of individuals has increased over recent years. It seems likely that this trend will continue in the future.
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 total fine amount has nearly doubled compared to the last ET Report, with the highest number of fines imposed in Spain (44) and Germany (23).

DPAs tend to treat bigger non-profit organisations (especially sports associations) just like similarly sized businesses. Fines were imposed for various aspects of non-compliance, ranging from insufficient technical and organisational measures to incompliant data subject information. For the smallest-sized controllers – i.e., individual entrepreneurs and private individuals – the DPAs apparently paid close attention to the extent to which the violation was foreseeable by the individual and to the purpose for the processing activity in question. The number of data subjects and the violator’s intention to pursue economic interests with 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 related to video surveillance / CCTV, including dashcams in private vehicles. DPAs consider CCTV a particular risky form of processing that even private individuals must meet strict requirements – notably if CCTV is operated in public areas.
We still assume that the protection of employee data will remain key field of activity for DPAs, considering the overall importance of its 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. On the other hand, employees may be more likely to raise complaints with a DPA, especially in case of conflict situations (including but not limited to cases ultimately brought to employment courts).

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 are increasingly exploiting legal 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. The established interpretation of such national employment laws usually influences the permitted extent of employee data processing.

A first analysis of employee data-related fines indicates that employer’s reliance on a statutory legal basis (such as performance of 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 2023), we highly appreciate any form of feedback (constructive is liked best…) and want to thank everybody who has reached out to us so far.

We received interesting thoughts, hints to forgotten fines (hidden deeply in remote corners of a supposedly completely captured world), recommendations for additional features (and our bucket 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

Luzia Esser, René Sandor, Fiona Savary, Alexander Schmid
E info@enforcementtracker.com

Enforcement Insights per business sector

Christoph Ceelen, Huy Do Chi, Anna Lena Fülsack, Felix Glocker,
Katharina Hirzle, Martin Kilgus, Martin Krings, Arne Schmieke

Enforcement Insights per country

Tom de Cordier, Francoise Billen, Anne-Laure Villedieu, Maxime Hanriot, Italo de Feo,
Mariangela Selvaggiuolo, Erik Jonkman, Ove Vanebo, Johannes Juranek, Christina Maria Schwaiger, Tomasz Koryzma,
Agnieszka Górecka, José Luis Piñar,
Javier Torre de Silva, Emma Burnett,
Loretta Pugh, Dóra Petrányi, Márton Domokos, Tomáš Matějovský, Daniel Szpyrc, Nevena Radlova, Maria Harizanova
### CMS Data Protection Contacts

<table>
<thead>
<tr>
<th>Country</th>
<th>Contact Name</th>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Albania</td>
<td>Mirko Daidone</td>
<td><a href="mailto:mirko.daidone@cms-aacs.com">mirko.daidone@cms-aacs.com</a></td>
</tr>
<tr>
<td>Algeria</td>
<td>Amine Sator</td>
<td><a href="mailto:amine.sator@cms-fl.com">amine.sator@cms-fl.com</a></td>
</tr>
<tr>
<td>Angola</td>
<td>Luís Borba Rodrigues</td>
<td><a href="mailto:luis.borbabarodrigues@lbr-legal.com">luis.borbabarodrigues@lbr-legal.com</a></td>
</tr>
<tr>
<td>Austria</td>
<td>Johannes Juranek</td>
<td><a href="mailto:johannes.juranek@cms-rrh.com">johannes.juranek@cms-rrh.com</a></td>
</tr>
<tr>
<td>Belgium</td>
<td>Tom de Cordier</td>
<td><a href="mailto:tom.decordier@cms-db.com">tom.decordier@cms-db.com</a></td>
</tr>
<tr>
<td>Bosnia and Herzegovina</td>
<td>Sanja Voloder</td>
<td><a href="mailto:sanja.voloder@cms-rrh.com">sanja.voloder@cms-rrh.com</a></td>
</tr>
<tr>
<td>Brazil</td>
<td>Ted Rhodes</td>
<td><a href="mailto:ted.rhodes@cms-cmno.com">ted.rhodes@cms-cmno.com</a></td>
</tr>
<tr>
<td>Bulgaria</td>
<td>Nevena Radlova</td>
<td><a href="mailto:nevena.radlova@cms-cmno.com">nevena.radlova@cms-cmno.com</a></td>
</tr>
<tr>
<td></td>
<td>Gentscho Pavlov</td>
<td><a href="mailto:gentscho.pavlov@cms-rrh.com">gentscho.pavlov@cms-rrh.com</a></td>
</tr>
<tr>
<td>Chile</td>
<td>Diego Rodriguez</td>
<td><a href="mailto:diego.rodriguez@cms-ca.com">diego.rodriguez@cms-ca.com</a></td>
</tr>
<tr>
<td>China</td>
<td>Nick Beckett</td>
<td><a href="mailto:nick.beckett@cms-cmno.com">nick.beckett@cms-cmno.com</a></td>
</tr>
<tr>
<td></td>
<td>Ulrike Glueck</td>
<td><a href="mailto:ulrike.glueck@cmslegal.cn">ulrike.glueck@cmslegal.cn</a></td>
</tr>
<tr>
<td>Colombia</td>
<td>Lorenzo Villegas-Carrasquilla</td>
<td><a href="mailto:lorenzo.villegas@cms-ra.com">lorenzo.villegas@cms-ra.com</a></td>
</tr>
<tr>
<td>Croatia</td>
<td>Marija Zrno</td>
<td><a href="mailto:marija.zrno@cms-rrh.com">marija.zrno@cms-rrh.com</a></td>
</tr>
<tr>
<td>Czech Republic</td>
<td>Tomas Matějovský</td>
<td><a href="mailto:tomas.matejovsky@cms-cmno.com">tomas.matejovsky@cms-cmno.com</a></td>
</tr>
<tr>
<td>France</td>
<td>Anne-Laure Villedieu</td>
<td><a href="mailto:anne-laure.villedieu@cms-fl.com">anne-laure.villedieu@cms-fl.com</a></td>
</tr>
<tr>
<td>Germany</td>
<td>Christian Runte</td>
<td><a href="mailto:christian.runte@cms-hs.com">christian.runte@cms-hs.com</a></td>
</tr>
<tr>
<td></td>
<td>Michael Kamps</td>
<td><a href="mailto:michael.kamps@cms-hs.com">michael.kamps@cms-hs.com</a></td>
</tr>
<tr>
<td>Hong Kong</td>
<td>Jonathan Chu</td>
<td><a href="mailto:jonathan.chu@cms-cmno.com">jonathan.chu@cms-cmno.com</a></td>
</tr>
<tr>
<td>Hungary</td>
<td>Dóra Petrányi</td>
<td><a href="mailto:dora.petranyi@cms-cmno.com">dora.petranyi@cms-cmno.com</a></td>
</tr>
<tr>
<td>Italy</td>
<td>Italo de Feo</td>
<td><a href="mailto:italo.defeo@cms-aacs.com">italo.defeo@cms-aacs.com</a></td>
</tr>
<tr>
<td>Kenya</td>
<td>Julius Wako</td>
<td><a href="mailto:julius.wako@cms-di.com">julius.wako@cms-di.com</a></td>
</tr>
<tr>
<td>Luxembourg</td>
<td>Vivian Walry</td>
<td><a href="mailto:vivian.walry@cms-dblux.com">vivian.walry@cms-dblux.com</a></td>
</tr>
<tr>
<td>North Macedonia</td>
<td>Marija Filipovska</td>
<td><a href="mailto:marija.filipovska@cms-rrh.com">marija.filipovska@cms-rrh.com</a></td>
</tr>
</tbody>
</table>
CMS Data Protection Contacts

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

**Monaco**  
Anne-Fleur Wagler  
E annefleur.wagler@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 jose.luis.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

**South Africa**  
Zaakir Mohamed  
E zaakir.mohamed@cms-rrm.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

**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
CMS Law-Now™

Your free online legal information service.

A subscription service for legal articles on a variety of topics delivered by email.
cms-lawnow.com

The sole purpose of this document is to provide information about specific topics. It makes no claims as to correctness or completeness and does not constitute legal advice. The information it contains is no substitute for specific legal advice. If you have any queries regarding the issues raised or other legal topics, please get in touch with your usual contact at CMS Hasche Sigle.

CMS Hasche Sigle is one of the leading commercial law firms. More than 600 lawyers serve their clients in eight major German commercial centres as well as in Beijing, Brussels, Hong Kong, and Shanghai. CMS Hasche Sigle is a member of CMS Legal Services EEBG, a European Economic Interest Grouping that coordinates an organisation of independent law firms. CMS EEBG provides no client services. Such services are solely provided by CMS EEBG’s member firms in their respective jurisdictions. CMS EEBG and each of its member firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS EEBG and each member firm are liable only for their own acts or omissions and not those of each other. The brand name “CMS” and the term “firm” are used to refer to some or all of the member firms or their offices.

CMS locations:

CMS Hasche Sigle Partnerschaft von Rechtsanwälten und Steuerberatern mbB, registered office: Berlin (Charlottenburg District Court, PR 316 B), list of partners: see website.
cms.law