


C L I F F O R D

C H A N C E



**EUROPEAN COURT OF JUSTICE IN FACEBOOK
RULING CLARIFIES INTERPLAY BETWEEN EU
COMPETITION LAW AND DATA PROTECTION
ENFORCEMENT, REINFORCES A HIGH BAR FOR
CERTAIN GDPR LEGAL BASES, AND CHALLENGES
RELIANCE ON LEGITIMATE INTERESTS FOR
DISCLOSURES TO LAW ENFORCEMENT AUTHORITIES**

EUROPEAN COURT OF JUSTICE IN FACEBOOK RULING CLARIFIES INTERPLAY BETWEEN EU COMPETITION LAW AND DATA PROTECTION ENFORCEMENT, REINFORCES A HIGH BAR FOR CERTAIN GDPR LEGAL BASES, AND CHALLENGES RELIANCE ON LEGITIMATE INTERESTS FOR DISCLOSURES TO LAW ENFORCEMENT AUTHORITIES

In *Case C-252/21 Meta Platforms Inc. and Ors v Bundeskartellamt*, handed down on 4 July 2023, the European Court of Justice (“**ECJ**”) clarified that an EU Member State competition authority may find a violation of the EU General Data Protection Regulation (“**GDPR**”), even where a data protection supervisory authority is investigating the same conduct, in the course of investigating an abuse of a dominant position under Article 102 of the Treaty on the Functioning of the European Union (“**TFEU**”). The Member State competition authority must cooperate closely with the competent EU Member State data protection supervisory authorities and is bound by their prior decisions. The ECJ also provided clarification on several important points of data protection law, including: (i) reinforcing the high bar required for reliance on the GDPR legal bases of consent, contractual necessity or the legitimate interests of the data controller; and (ii) ruling out reliance on the legitimate interests of the data controller for disclosures of personal data to law enforcement agencies for prevention, detection and prosecution of criminal offences.

Key takeaways and practical implications

1. Competition authorities in the EU can assess a breach of EU data protection rules where necessary to determine the existence of an abuse of dominant position. The competition authorities must cooperate with the relevant data protection authorities and are bound by any previous decisions of those authorities in relation to the conduct being examined
2. Dominance of the service provider in the market, while not determinative, is a circumstance that must be taken into consideration in assessing whether the user of that service has freely given consent under the GDPR. It can create an imbalance between the user and social network provider and can affect whether consent can be withheld or withdrawn without detriment. Although the judgment strictly only opines about providers of social network services, the same reasoning would appear to apply to data processing by providers of other dominant online services.

3. Processing of (non-special category) personal data can be justified on the basis that it is necessary for the performance of a contract only where the processing is 'objectively indispensable' for performance of the contract (interpreted strictly). Providing personalised content online, while useful to the user, *"does not appear to be necessary"* to offer users the services of the online social network as it can be provided to the user in the form of an *"equivalent alternative...which does not involve such a personalisation"*.
4. In the context of the creation of user profiles for targeted online advertising, a controller cannot rely on the GDPR legal basis that processing is necessary for the purposes of their legitimate interests where the scale and intrusiveness of the processing go beyond a user's reasonable expectations. Taken together with the high bar required for consent and strict interpretation of contractual necessity, this could create challenges for certain targeted online advertising practices.
5. Controllers cannot (as a matter of principle) rely on their legitimate interests as a GDPR legal basis for disclosure of personal data to law enforcement agencies for the purposes of the prevention, detection and prosecution of criminal offences. This is particularly challenging for disclosures to law enforcement agencies in third countries. The judgment is silent on the possibility of reliance on the data recipient's (the law enforcement agency's) legitimate interests or reliance on Article 6(1)(e) GDPR (public interest) – both of which are untested law.
6. As a user's online activity can involve special category data under the GDPR (relating, e.g., to health or religion), the processing of data regarding this activity (such as website visits) on the basis that it has been manifestly made public requires clear affirmative action indicating intent by the individual to make the data relating to him or her publicly accessible to an unlimited number of persons.

Background to the case

GDPR and data processing

Where caught within its territorial scope, the GDPR sets out certain legal bases that a data controller must rely on when processing personal data. These are outlined in Article 6(1)(a)-(f) GDPR. For example, a data controller may process data in a specific way where a data subject gives their consent for their personal data to be processed in that way.

The GDPR also strictly regulates the processing of particularly sensitive personal data, known as 'special categories of personal data', such as a person's ethnic origin or sexual orientation. As a general rule, the processing of such data is unlawful unless a data controller can rely on limited exceptions, outlined in Article 9(2) GDPR such as the fact that a data subject has made the special category of personal data public.

As a result of wider territorial scope provisions of the GDPR, Facebook is subject to the GDPR in relation to its users within the European Economic Area ("**EEA**"). The data protection supervisory authority of the Member State in which a controller is deemed to have its main establishment within the EEA leads this enforcement, although there are exceptions.

The German Facebook data antitrust case triggering the preliminary questions to the ECJ

In 2019, the German Federal Cartel Office (“**FCO**”) in a highly publicized decision found that Meta (then known as Facebook) had abused its dominant position in the market for private social networks in Germany, in violation of EU and German antitrust law.

Meta’s advertising-funded services collect large volumes of data from its users and combine these into user profiles for advertising purposes. The FCO found that Meta was exploiting users of the Facebook private social network (“**Facebook**”) by having them agree to combining their personal data with data that Meta collected through its tracking cookies from other Meta services and third-party websites or apps (“**off-Facebook data**”). Facebook users had to agree to this combination of data when clicking on the ‘sign up’ button, accepting Facebook’s general terms and privacy policy, in order to gain access to any of Meta’s services.

The FCO determined that Facebook was dominant in the market for private social networks in Germany. The FCO relied on German case law that outlined that it may review terms as potentially abusive where those terms are imposed as a manifestation of market power and infringe a party’s civil or constitutional rights. In application of this precedent, the FCO held that it could determine whether Facebook’s privacy policy (which set out terms regarding users’ fundamental right to privacy) infringed the privacy rights of its users and constituted a manifestation of market power on the part of Meta. In the reasoning of the FCO, data protection compliance was a key element to determining whether Meta abused its dominance under antitrust law by imposing exacting data collection and combination terms.

On that basis, and after liaising closely with the data protection supervisory authority in Germany and the lead data protection supervisory authority in Ireland, the FCO found that Meta was in breach of the GDPR because its collection and combining of user data was not lawful. The FCO found that Meta could not rely on any of the lawful processing grounds under the GDPR for this practice. Users did not validly consent to the collection and combination of their data as they were not given a free choice: among other reasons, users consented to Facebook’s terms and conditions for the sole purpose of concluding the contract and using Facebook’s services (Article 6(1)(a) GDPR). Meta could not claim that such processing was necessary for the performance of the contract of providing private social network services (Article 6(1)(b) GDPR), Meta equally could not rely on the relevant data processing being necessary for the purposes of its legitimate interests (Article 6(1)(f) GDPR). Finally, none of the other grounds under Article 6(1) GDPR applied (such as compliance with legal obligations).

The FCO ordered Meta to implement necessary changes to its data handling procedures and stop the relevant combination of user data unless consent for such combination was freely given.

Meta lost its bid to have the FCO decision stayed in interim relief proceedings litigated to the highest German court, the Federal State Court. Meta also challenged the FCO’s decision on the merits before the Higher Regional Court of Düsseldorf (the “**Düsseldorf Court**”). Among other things, Meta objected to the FCO’s GDPR infringement determination despite GDPR enforcement being entrusted to data protection supervisory authorities (and specifically, the lead authority in Ireland). Meta also

contested the FCO's assessment of Meta's GDPR compliance, including the validity of alternative legal bases to consent for its processing. The Düsseldorf Court requested a preliminary ruling from the ECJ on these issues, which raised questions regarding the interpretation of the GDPR and the interplay between data protection and antitrust enforcement.

The questions that the Düsseldorf Court asked regarding antitrust were: (i) whether a Member State competition authority, which is not a data protection supervisory authority and which is not located in the Member State where the company has its main establishment, may find a breach of the GDPR when investigating abuses of competition law; and (ii) whether valid consent can be given to a dominant undertaking such as Meta for the processing of data.

The Düsseldorf Court also asked questions of interpretation of the GDPR: (iii) whether Meta's collection of data from third-party websites relating to sensitive data categories (e.g., regarding health or religion), and including it into a user's profile constitutes processing of special categories of data within the meaning of Article 9 GDPR; (iv) whether the processing of special categories of data may be justified on the basis that the sensitive data was made manifestly public by the data subject (Article 9(2)(e) GDPR) in circumstances where a user visits or uses a website or app; and (v) whether Meta can justify the collection and processing of off-Facebook data on the ground of necessity of performance of the contract (Article 6(1)(b) GDPR) or the pursuit of legitimate interests (Article 6(1)(f) GDPR).

Findings of the ECJ

1. Member State competition authorities have the power to review GDPR compliance if necessary to establish abuse, subject to collaborating with relevant data protection supervisory authorities

The ECJ recalled that Member State competition authorities must assess, based on all the specific circumstances of the case, whether conduct is abusive or not. To that end, the ECJ held that access to personal data has become a significant parameter of competition between undertakings and is thus relevant for Member State competition authorities to take into consideration when examining a potential abuse of a dominant position. The ECJ concluded that the compliance or non-compliance with the GDPR can be a "vital clue" among the circumstances of the case to establish whether certain conduct is anticompetitive. The ECJ did not go as far as to say that the finding of a GDPR non-compliance can be tantamount to an abuse, or that it is required for a finding of infringement in abuses involving data collection and combination, and does not require Member State competition authorities to consider data protection compliance in developing theories of harm involving personal data.

The ECJ held that a Member State competition authority can therefore determine whether an undertaking is in breach of the GDPR in the context of establishing an abuse of dominance. However, a Member State competition authority must cooperate with the competent data protection supervisory authorities to ensure the consistency of application of the GDPR. A Member State competition authority cannot depart from a decision by the relevant data protection supervisory authorities although it remains free to draw its own conclusions from the point of view of the application of competition law. If no decision has yet been issued, the Member State competition authority must consult with the relevant data protection supervisory authorities prior to proceeding.

The judgment underscores that, where a Member State competition authority finds non-compliance with GDPR in the process of establishing an abuse, it does not replace the role of the data protection supervisory authorities. The sole purpose of the assessment of compliance with GDPR by a Member State competition authority is to establish an abuse of a dominant position and impose measures to end that abuse. As such, dominant undertakings could find themselves open to separate (parallel) investigations by both Member State competition authorities and data protection supervisory authorities where GDPR compliance could be at the forefront.

2. Whilst a service provider's dominant position in a market is not determinative in assessing the validity of consent under the GDPR, it is a circumstance that must be taken into consideration, with the onus being on the dominant undertaking to demonstrate that consent was freely given

The ECJ held that the fact an operator of an online social network holds a dominant position on the social network market does not, as such, prevent its users from validly giving their consent (within the meaning of the GDPR) to the processing of their personal data. However, the ECJ pointed out that *“such a circumstance must be taken into consideration in assessing whether the user of that network has validly and, in particular, freely given consent, since that circumstance is liable to affect the freedom of choice of that user, who might be unable to refuse or withdraw consent without detriment.”* The ECJ specifically referred to: (i) the consequences of being unable to refuse or withdraw consent without detriment (such as the underlying service no longer being provided); (ii) the importance of considering whether there is a clear imbalance between the data subject and the controller; and (iii) whether the processing does not allow separate consent to be given to different personal data processing operations despite separate consents being appropriate in the circumstances. The ECJ also highlighted the issue of making the performance of a contract, including the provision of a service, conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

3. The processing of a user's data derived from their actions on third-party websites from which special categories of personal data could be derived can constitute processing of special categories of personal data

The ECJ found that Meta collects personal data from users' on- and off-platform website and app visits, and from information they fill in there, and then links that information to users' social media accounts and uses that information to target advertising. The ECJ concluded that this process could involve “processing of special categories of personal data” within the meaning of Article 9(1) GDPR where the data relates to sites or apps where special category of data could be generated e.g., dating websites where a user visits such a website and fills information on those sites.

4. Clear affirmative action by the data subject is needed in order for an online provider to be able to process online user activity data constituting special category personal data on the basis that it was manifestly made public

In such cases, the ECJ examined whether the derogation from Art. 9(2)(e) GDPR (allowing the processing of sensitive data that has been manifestly made public by the data subject) could be applicable. The ECJ reasoned that, when a user visits or submits information to third-party websites and apps relating to special categories of

personal data, they do not *intend* (explicitly and by a clear and affirmative action with full knowledge of the facts) to make public (i.e., accessible to the general public / an unlimited number of persons) the fact that they visited those sites or apps or any personal data revealed by their interaction with those sites or apps. It found that a “mere visit” to such websites or apps by a user does not mean that personal data is manifestly made public by that user within the meaning Article 9(2)(e) GDPR and that such intention cannot be inferred merely by interacting with a website. The ECJ also noted that whether the interactions of a user, such as clicking on integrated buttons (“Like”, “Share”, etc.) or actually entering information, could be justified as the user making public their personal data, must be viewed in light of individual privacy settings.

Where individual privacy settings are available, and the user entered information on the basis of individual privacy settings providing for access of user data to an unlimited number of persons and selected with full knowledge of the facts, those users have clearly made the choice to have the personal data made public. Where individual privacy settings are unavailable, data subjects must have explicitly consented to the personal data being viewed by anyone having access to that website or app. In effect, this calls into question whether it would ever be possible to process special category data gleaned from third-party websites / apps (absent explicit consent), and places severe constraints on a social media network in relation to the processing of special category data on its own website (absent a user’s privacy settings being set to ‘anyone’, or similar).

5. Processing of data can be justified on the basis that it is necessary for the performance of a contract only where the processing is ‘objectively indispensable’ for performance of the contract, which the ECJ suggested was unlikely in the case of offering personalised content on a social network

Article 6(1)(b) GDPR provides that processing of personal data is lawful if it is “*necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*”. The ECJ interprets this basis for processing narrowly. It ruled that the necessity element is fulfilled where it is objectively indispensable for a purpose that is integral to the contractual obligation intended for the data subject. The data controller must therefore be able to demonstrate how the main subject matter of the contract cannot be achieved if the processing in question does not occur and that there are no workable, less intrusive alternatives. Where the contract consists of several separate services or elements of a service that can be performed independently of one another, the necessity requirement should be assessed in the context of each of those services separately.

The ECJ considered whether the provision of personalised content justified the processing of personal data in reliance on the “performance of a contract” basis. It concluded that personalised content “*is useful to the user*”, but that it “*does not appear to be necessary*” in order to offer users the services of the online social network. The ECJ added that such personalised content may be provided to the user in the form of an “*equivalent alternative...which does not involve such a personalisation, such that the latter is not objectively indispensable for a purpose that is integral to those services.*”

The ECJ also considered whether the processing of personal data of services offered by the Meta group's own services, other than the relevant online social network service, was necessary. The ECJ remarked that the various products and services offered by that group can be used independently of each other and the use of each product or service is based on the conclusion of a separate user agreement. Therefore, the processing of personal data from other services offered by the Meta group, other than the relevant online social network service, did not appear to the ECJ to be necessary for the online social network service to be provided, but this necessity was ultimately for the Düsseldorf Court to determine.

The ECJ's narrow interpretation of the concept of "contractual necessity" of personalised content follows a long line of authority. First, this interpretation is in line with that the view already adopted by the European Data Protection Board ("**EDPB**") in binding decisions 3/2022 and 4/2022 regarding Meta's legal basis for personalised advertising (an interpretation that Meta is currently challenging before the EU General Court for being overly narrow). The interpretation is also in line with the EDPB's guidelines on the topic, binding decisions adopted in the context of dispute resolution mechanisms and decisions from EU authorities finding that processing for purposes of personalised advertising to the extent engaged in by some online players is not "objectively necessary" for the purpose of providing online services such as social network services.

6. There are significant restrictions on the use of legitimate interests as a basis for processing user data under the GDPR, which have broad implications beyond social media

The legitimate interest legal basis applies only when processing is clearly communicated to users, is proportionate, and, in any event, not overridden by users' fundamental rights in the specific case, which the ECJ questioned in the case of Meta.

Article 6(1)(f) GDPR provides that processing of personal data is lawful if it is "*necessary for the purposes of the legitimate interests pursued by the controller or by a third party*" (subject to some exceptions).

In the case at hand, the legitimate interests pursued by Meta through the data processing were, inter alia: (i) personalised advertising; (ii) ensuring network security; (iii) product improvement; and (iv) disclosures to law enforcement agencies in order to prevent, detect and prosecute criminal offences.

First, with regards to personalised advertising, the ECJ recalled that Recital 47 GDPR provided that the processing of personal data for direct marketing purposes may be regarded as a legitimate interest. However, concerning the balancing test, the ECJ noted that the processing carried out by Meta "*is particularly extensive since it relates to potentially unlimited data and has a significant impact on the user, a large part – if not almost all – of whose online activities are monitored by Meta Platforms Ireland, which may give rise to the feeling that his or her private life is being continuously monitored*".

The ECJ reasoned that, despite the fact that the services of an online social network such as Facebook are free of charge, the user of that network cannot “*reasonably expect*” that Facebook would process their personal data (without their consent) for the purposes of personalised advertising. In such circumstances, given the large scale and intrusiveness of the processing at hand for users, it must be held that the interests and fundamental rights of the user override the interest of that operator in such personalised advertising. Therefore, the processing cannot be justified on the basis of Article 6(1)(f) GDPR.

Second, regarding the objective of ensuring network security, that objective, as stated in Recital 49 GDPR, constitutes a legitimate interest capable of justifying the processing. However, the ECJ left it to the referring Düsseldorf Court to ascertain whether, and to what extent, the processing of personal data collected from third-party sources is actually necessary to ensure that the internal security of that network is not compromised.

Third, as regards the product improvement objective, the ECJ similarly doubted whether the product improvement objective can override the interests and fundamental rights of the user, given the large scale of the processing and its significant impact on users and, again, given that the user cannot reasonably expect such data to be processed by Meta without the user’s consent.

Fourth, in relation to information sharing with law enforcement agencies in order to prevent, detect and prosecute criminal offences, the ECJ held that this objective was not capable (as a matter of principle) of constituting a legitimate interest pursued by the controller, as it is unrelated to the controller’s economic and commercial activity. This was not expected, as the 2019 joint letter from the European Data Protection Board and European Data Protection Supervisor to the LIBE Committee, whilst casting doubt on whether certain disclosures of personal data to U.S. law enforcement agencies would be able to rely on the controller’s legitimate interests as the lawful basis of processing (due to specific facts relating to the Stored Communications Act and CLOUD Act), did not altogether rule it out as a matter of principle.

This has implications wider than social networks: Many large organisations that are dually regulated by European data protection laws and the laws of third countries mandating disclose personal data to third country law enforcement agencies have historically relied upon their legitimate interest under Article 6(1)(f) GDPR when making such disclosures (given that Article 6(1)(c) – compliance with a legal obligation to which the controller is subject – is strictly limited to EU or Member State legal obligations and not those of a third country).

It remains to be seen whether there is any scope in arguing that the processing is necessary for the legitimate interests of the third party recipient namely the law enforcement agency) under Article 6(1)(f) GDPR, or even whether Article 6(1)(e) (public interest) has a role to play. In both cases, this is untested law.

Takeaways and next steps for the German case

The case is far from settled. Although the ECJ judgment is favourable to the FCO's position, the Düsseldorf Court will now need to rule on the substance by applying the ECJ's answers to the facts and also deciding arguments that were not the subject of the preliminary ruling to the ECJ.

While we will have to await the Düsseldorf Court's decision on the merits of Meta's appeal, the President of the FCO, Andreas Mundt, has already stated publicly that the FCO will continue to *"investigate...and try to limit the collection of data and the merging of data... The judgment will influence the business model of Big Tech. There is a lot of space for further proceedings. Let's see how we go about that."*¹

The judgment overall is favourable to competition enforcers seeking to address dominant digital players' data collection, combination and user profiling practices through competition law, and the outcome will embolden European competition authorities to proceed further down this path.

At the same time, the ECJ's GDPR findings are not confined to the practices of dominant companies. The ECJ's judgment signals to online service providers that consent as a basis for data processing must truly be freely given, and that reliance on alternative grounds such as legitimate interest and performance of the contract will not pass muster if the relevant data processing terms merely pay lip service to the processing necessity requirement, or where the fundamental rights and interests of users in their privacy outweigh the interests of the data controller. This approach is not fundamentally new, as it is consistent with that taken by the EDPB and national data protection supervisory authorities.

What is new, with potentially far-reaching consequences, is the finding that, in principle, a controller cannot be considered as having a legitimate interest in disclosing personal data to law enforcement agencies for the prevention, detection and prosecution of criminal offences.

Companies regulated by the GDPR which are impacted by the judgement may need to reconsider their legal basis analysis and review associated records, policies and processes.

¹ <https://content.mlex.com/#/content/1482356/antitrust-watchdogs-can-invoke-gdpr-violations-as-part-of-competition-probes-eu-court-rules>

AUTHORS



Dieter Paemen
Partner
Brussels
T: +32 2 533 5012
E: dieter.paemen@cliffordchance.com



Simon Persoff
Partner
London
T: +44 207006 306
E: simon.persoff@cliffordchance.com



Paschalis Lois
Lawyer
Brussels
T: +32 2 533 5906
E: paschalis.lois@cliffordchance.com



Holger Lutz
Partner
Frankfurt
T: +49 69 7199 1670
E: holger.lutz@cliffordchance.com



Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com



Michael Dietrich
Partner
Düsseldorf
T: +49 211 4355 5542
E: michael.dietrich@cliffordchance.com



Samantha Ward
Partner
London
T: +44 207006 8546
E: samantha.ward@cliffordchance.com



Carmen Puscas
Lawyer
Brussels
T: +32 2 533 5094
E: carmen.puscas@cliffordchance.com



Oscar Tang
Senior Associate
London
T: +44 207006 3749
E: oscar.tang@cliffordchance.com



Alexandre Balducci
Avocat
Paris
T: +33 1 4405 5137
E: alexandre.balducci@cliffordchance.com



Shruti Hiremath
Senior Associate
London
T: +44 207006 3075
E: shruti.hiremath@cliffordchance.com



Rita Flakoll
Global Head of Tech Group Knowledge
London
T: +44 207006 1826
E: rita.flakoll@cliffordchance.com

CONTACTS



Jonathan Kewley
Partner
London
T: +44 207006 3629
E: jonathan.kewley@cliffordchance.com



Devika Kornbacher
Partner
Houston
T: +1 713 821 2818
E: devika.kornbacher@cliffordchance.com



Stella Cramer
Partner
Singapore
T: +65 6410 2208
E: stella.cramer@cliffordchance.com



Ashwin van Rooijen
Partner
Brussels
T: +32 2 533 5091
E: ashwin.vanrooijen@cliffordchance.com



Marc Besen
Partner
Düsseldorf
T: +49 211 4355 5312
E: marc.besen@cliffordchance.com



Sharis Pozen
Regional Managing Partner Americas
Washington, D.C.
T: +1 202 912 5226
E: sharis.pozen@cliffordchance.com



Gunnar Sachs
Partner
Düsseldorf
T: +49 211 4355 5460
E: gunnar.sachs@cliffordchance.com



Fernando Irurzun
Partner
Madrid
T: +34 91 590 4120
E: fernando.irurzun@cliffordchance.com



Katrin Schallenberg
Partner
Paris
T: +33 1 4405 2457
E: katrin.schallenberg@cliffordchance.com



Milena Robotham
Partner
Brussels
T: +32 2 533 5074
E: milena.robotham@cliffordchance.com



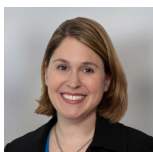
Nelson Jung
Partner
London
T: +44 207006 6675
E: nelson.jung@cliffordchance.com



Jennifer Storey
Partner
London
T: +44 207006 8482
E: jennifer.storey@cliffordchance.com



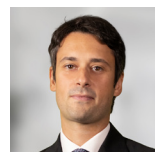
Stavroula Vryna
Partner
London
T: +44 207006 4106
E: stavroula.vryna@cliffordchance.com



Megan Gordon
Partner
Washington, D.C.
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com



Jaap Tempelman
Senior Counsel,
Amsterdam Tech Group Co-Head
T: +31 20 711 9192
E: jaap.tempelman@cliffordchance.com



Andrea Tuninetti
Ferrari
Lawyer - Counsel
Milan
T: +39 02 8063 4435
E: andrea.tuninettiferrari@cliffordchance.com



Andrei Mikes
Counsel
Amsterdam
T: +31 20 711 9507
E: andrei.mikes@cliffordchance.com



Grégory Sroussi
Counsel
Paris
T: +33 1 4405 5248
E: gregory.sroussi@cliffordchance.com

C L I F F O R D C H A N C E

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2023

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.