August 2023

VBB on Belgian Business Law

Issue Highlights

"Van Bael & Bellis' Belgian competition law practice [...] is a well-established force in high-stakes, reputationally-sensitive antitrust investigations."

Legal 500, 2019

Topics covered in this issue

vbb@vbb.com
www.vbb.com

Table of contents

Chaussée de La Hulpe 166
Terhulpsesteenweg
B-1170 Brussels – Belgium

Phone: +32 (0)2 647 73 50
Fax: +32 (0)2 640 64 99

vbb@vbb.com
www.vbb.com

COMPETITION LAW

Chief Prosecutor Damien Gerard Takes Public Stance on Role, Challenges and Prospects of Belgian Competition Authority

Damien Gerard, the Chief prosecutor (*Auditeur-generaal / Auditeur general*) of the Belgian Competition Authority (*Belgische Mededingingsautoriteit / Autorité belge de la Concurrence* – the ***BCA***) gave an interview to the competition law magazine Concurrences. In this interview, published on 23 August 2023, Damien Gerard discusses the role of the BCA as enforcer of the competition rules, the social and environmental challenges which the BCA is currently facing, and his views on how to achieve "*a rigorous and effective competition policy anchored in market realities*".

Merger Control

Regarding merger control, Mr. Gerard starts by stressing the need for competition authorities to root their analysis in market realities rather than in arguments, anecdotes, projections or assumptions, especially if these are only supported by transaction-specific materials. Instead, competition authorities should rely, for example, on internal documents produced in the normal course of business and use substantive concepts and procedural and remedial tools as far as possible within the applicable legal limits.

Mr. Gerard also believes that the application of Article 102 TFEU to non-notifiable concentrations will remain residual and limited to cases falling within the scope of the *Towercast* (C-449/21) judgment. Similarly, Mr. Gerard considers that the referral mechanism provided for by Article 22 of Regulation No 139/2004 of 20 January 2004 on the control of concentrations between undertakings is used "*sparingly, in appropriate cases only*". Yet, this does not mean that there is a "lawless zone" below the notification thresholds. On the contrary, Mr. Gerard points to the ongoing *Proximus / EDPNet* case as an example of "*the need to retain the possibility to act decisively when the circumstances warrant it*".

Cartels

As regards cartels, Mr. Gerard announces that dawn raids, which were suspended during the Covid-19 pandemic, are now "*certainly back on the agenda*". However, they should now reflect the various challenges resulting from (i) the multiplication of communication channels; (ii) the surge in digital information; and (iii) the more frequent reliance on searches in private homes. Mr. Gerard adds that the BCA's whistleblowing tool which was set up half a year ago "*has already demonstrated its usefulness in antitrust but also in merger control cases*" and will be more widely advertised further to the transposition of the Whistleblower Directive.

Mr. Gerard adds that he "*consciously identified a number of priority cases and ring-fenced people and resources to get them done*". He mentions cases regarding "*bid rigging, no-poaching* [and] *category management*", which "*have now reached the stage of formal objections or are close to a decision*". This statement may refer in part to the BCA's recent announcement that a Statement of Objections was sent to G4S, Securitas and Seris on account of bid rigging and no-poaching arrangements in the private security sector (*See*, this Newsletter, Volume 2023, No. 7).

On climate issues, Mr. Gerard points out that competition law compliance of sustainability initiatives is constantly being discussed at the level of national competition authorities, including the BCA.

Informal Advice

Mr. Gerard also emphasises the importance of informal discussions between the Prosecution and Investigation Service of the BCA and business, as he stresses that the BCA being aware of a situation before it is reported by a third party "*can have a real impact on the way it will be dealt with subsequently*". Mr. Gerard therefore

COMPETITION LAW

encourages companies "*to be genuinely open and approach* [the BCA] *as a mature and trusted partner, committed to doing the right thing instead of seeking to engage in formal enforcement actions at all costs*."

Abuse of Economic Dependence

Finally, Mr. Gerard announces that the BCA is "*investigating actively*" a few cases of abuse of economic dependence "*in the hope of establishing a few meaningful precedents*". However, he stresses that such cases "*are not going to overtake antitrust action any time soon*", considering their enforcement difficulty. First, economic dependence takes place between identifiable market players who are dependent on each other, which can give rise to problems of disclosure, confidentiality, fear of reprisals and reputational risk. Second, Mr. Gerard considers that courts and tribunals are "*often best placed to provide redress*" when companies suffer harm resulting from a deteriorated or broken business relationship. Finally, competition authorities have to establish the effect on competition, which may be difficult when the plaintiff does not have a strong market position.

Brussels Court Dismisses Football Club Virton's Request to be Readmitted to Second-Tier Professional League in Battle Involving Foreign Subsidies

On 10 August 2023, the Dutch-language Court of First Instance of Brussels (***Court of First Instance***) dismissed as inadmissible the request made by football club Royal Excelsior Virton (***Virton***) to be readmitted to Belgium's second-tier professional league.

It is not the first time that Virton fights in court to avoid or undo the results of relegation (*See*, this Newsletter, Volume 2020, No. 11). On this occasion, Virton contends that competing football club SK Lommel (***Lommel***) had received capital injections from the Emirate of Abu Dhabi, which it believes violates competition law and Regulation 2022/2560 on foreign subsidies distorting the internal market (*Foreign Subsidies Regulation* – the ***FSR***). According to Virton, these illegal foreign subsidies had a significant impact on sporting developments in the 2022-2023 season.

Procedure before Belgian Court of Arbitration

Virton initially brought a case before the Belgian Court of Arbitration (*Belgisch Arbitragehof voor de Sport / Cour belge d'Arbitrage pour le Sport* – the ***COA***) to deny Lommel a licence to participate in the second-tier professional league. Virton argued that there were serious indications that Lommel is structurally financed by foreign subsidies within the meaning of the FSR, and that, absent these foreign subsidies, Lommel would not have satisfied the licensing criteria.

The COA observed that, while the FSR had entered into effect on 12 January 2023, it only became applicable on 12 July 2023. The COA also noted that the European Commission is exclusively competent to rule on the application of the FSR, which does not have direct effect. Finally, the COA rejected Virton's claim that Lommel had also infringed Article 101 TFEU.

Procedure before Brussels Court of First Instance

Virton not only appealed the COA's decision. It also filed a complaint urging the European Commission to exercise its exclusive jurisdiction to enforce the FSR.

While waiting for the outcome of these procedures, and because it needed a remedy before the beginning of the football season that started on 11 August 2023, Virton sought interim measures from the Court of First Instance and requested to be included as the 17th team in the league. However, the Court of First Instance observed that Virton's claim was based on the same facts and had the same purpose as the previous arbitral decision of the COA. As a result, the Court of First Instance held that it could not grant the requested interim measure without flouting the character of res judicata of the arbitral decision.

LaLiga Complaint against Paris Saint-Germain

Virton is not the only club seeking redress based on the FSR. The Spanish football league, LaLiga, recently filed a complaint with the European Commission concerning the Qatari backing of the football club Paris Saint-Germain (***PSG***). LaLiga asserts that the French club

COMPETITION LAW

benefitted from foreign subsidies provided by the State of Qatar and allegedly resulting in significant imbalances in various national football leagues. According to LaLiga, PSG uses unlawful foreign subsidies to secure the services of top-tier players and coaches.

The cases of Virton and LaLiga represent an early test for the FSR. These complaints raise important questions about the extent to which non-EU state aid should be allowed in professional football and whether this creates unfair advantages.

CONSUMER LAW

New Consumer Debt Collection Rules Enter into Force – Update Your General Terms and Conditions Now

On 1 September 2023, the Law of 4 May 2023 inserting Book XIX "Consumer debts" into the Belgian Code of Economic Law entered into force for consumer contracts which were concluded on or after that date (*Wet van 4 mei 2023 houdende invoeging van boek XIX "Schulden van de consument" in het Wetboek van Economisch Recht / Loi du 4 mai 2023 portant insertion du livre XIX "Dettes du consommateur" dans le Code de droit économique* – the ***Law***). As of 1 December 2023, the Law will also apply to the recovery of consumer debts from contracts concluded before 1 September 2023 if the delay in payment or the amicable recovery occurs after 1 September 2023.

The primary objective of the Law is to modernise the rules governing the amicable recovery of consumer debts, whether by the creditor or through third-party intermediaries. In addition, the federal Parliament aims to strike a balance between the adverse effects encountered by companies resulting from late payments by consumers and the financial impact on consumers of debt collection activities (*See also*, this Newsletter, Volume 2023, No. 4 and Volume 2022, No. 10).

Free First Reminder and 14-day Grace Period

If consumers fail to pay their debts by the due date and a penalty clause applies, the application of this clause will be subject to (i) the issuance of a formal notice (taking the form of a first reminder); and (ii) the expiry of a grace period of at least 14 calendar days starting from the third working day after sending the reminder. If the reminder is sent electronically, the 14-day grace period starts on the calendar day following the day of sending of the first reminder.

The costs of the first reminder cannot be charged to the consumer. As regards contracts for the regular supply of goods or services, reminders pertaining to three expired due dates within a given calendar year should be free of charge for the consumer. The costs of additional reminders must not exceed EUR 7.50, to be increased with the postal charges applicable at the time of sending.

Capped Interests and Penalty Clauses

If consumers fail to pay the outstanding debt within the 14-day grace period, creditors may claim interest and late payment damages under a contractual penalty clause. However, to prevent these amounts from being disproportionate with the actual damage incurred, the Law applies a ceiling to both the interest rates and the amount of possible damages:

- The interest must be based on the outstanding amount and will be capped at the rate provided for in Article 5 of the Law of 2 August 2002 on combating late payment in commercial transactions (*Wet van 2 augustus 2002 betreffende de bestrijding van de betalingsachterstand bij handelstransacties / Loi du 2 août 2002 concernant la lutte contre le retard de paiement dans les transactions commerciales*). This interest rate is updated every six months.

- The damages must be proportionate with the amount of the outstanding debt. Debts equal to or lower than EUR 150 entitle the creditor to a maximum compensation of EUR 20. If the outstanding amount ranges between EUR 150.01 and EUR 500, the maximum compensation is set at EUR 30, to be increased by 10% of the outstanding amount between EUR 150.01 and EUR 500. If the outstanding amount exceeds EUR 500, the compensation is capped at EUR 65, to be increased by 5% of the outstanding amount exceeding EUR 500, subject to an overall cap of EUR 2,000.

Businesses are well advised to amend and update their general terms and conditions now. Any terms and conditions that diverge from the Law will be considered null and void.

The Law is available here (in Dutch) and here (in French).

CORPORATE LAW

Federal Public Service Finance Warns of Requirement to Ensure Correct Registration of Corporate Details in Ultimate Beneficial Owner Register

On 16 August 2023, the Federal Public Service Finance (***FPS Finance***) announced that it had abandoned its indulgent attitude towards incorrect registrations and a lack of entry in the Belgian Register for ultimate beneficial owners (the ***UBO Register***). FPS Finance reminded stakeholders that the deadline for completing the UBO registration was 30 September 2019 (and one month following a subsequent incorporation of a legal entity).

While FPS Finance mentioned that it had already issued fines in November 2021 and December 2022, it applied a period of tolerance for firms which had taken care of their UBO registration while failing to follow the correct procedure. This tolerance period has now ended.

The UBO Register was introduced in Belgium as part of the implementation of the fourth anti money laundering Directive 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (*See*, this Newsletter, Volume 2017, No. 8). The regulatory framework of the UBO Register was further defined in the Royal Decree of 30 July 2018 regarding the functioning of the UBO Register (the ***Decree***), which specifies the information regarding the ultimate beneficial owner(s) of the specific entities that must be registered in the UBO Register (*See*, this Newsletter, Volume 2018, No. 8) and the Royal Decree of 23 September 2020 amending the Decree, which created the obligation to submit supporting documents demonstrating that the registered information is sufficient, accurate and correct (*See*, this Newsletter, Volume 2020, No. 10).

The announcement of FPS Finance of 16 August 2023 can be found here (in Dutch) and here (in French). Further information on how to perform UBO registrations can be found in the guidelines of FPS Finance, accessible here (in Dutch) and here (in French).

DATA PROTECTION

European Commission Proposes Improvements to Cross-Border Enforcement of General Data Protection Regulation

On 4 July 2023, the European Commission (***Commission***) published its proposal for a Procedural Regulation to complement the General Data Protection Regulation (***GDPR***) with regard to the enforcement of EU data protection law in cross-border cases (***Proposal***). The Proposal does not alter the GDPR, but rather fleshes out the procedural rights to which parties to proceedings are entitled. It also harmonises cooperation by concerned supervisory authorities (***CSAs***) under the One-Stop-Shop (***OSS***) mechanism.

For controllers and processors, the most relevant elements of the Proposal are the right to be heard, the right to access the documents of the proceedings, and the streamlining of the decision-making process before the European Data Protection Board (***EDPB***).

The Proposal specifically governs cross-border processing which, according to Article 4(23) GDPR involves the processing of personal data in the context of activities of establishments or data subjects in more than one Member State.

Right to Be Heard for Parties under Investigation

The Proposal provides that prior to adopting its Binding Decision, the Chair of the EDPB will, through the lead supervisory authority (***LSA***), provide the parties with a statement of reasons explaining the reasoning which the EDPB intends to adopt. The period within which the party under investigation is requested to comment on the statement of reasons is short (1 week) and the Proposal would not grant that party a right to an oral hearing.

Improved Access to File and Additional Confidentiality Provisions

The Proposal grants parties under investigation access to file after preliminary findings are notified. The LSA will only be able to rely on the documents that support the preliminary findings on which the parties had the opportunity to comment.

The Proposal also defines measures to protect privileged information and allows the parties to identify and seek protection for confidential elements.

Submission of Comments and Relevant Objections

Currently, CSAs submit so-called reasoned and relevant objections (***RROs***) and comments after receiving the LSA's Draft Decision. To facilitate cooperation and agreement between DPAs, the Proposal allows CSAs to send comments much earlier during the procedure.

The Proposal also contains detailed requirements for the form and structure of RROs. Article 18 of the Proposal indicates that RROs must be confined to factual elements included in the Draft Decision, and they cannot change the scope of the investigation by raising possible additional infringements of the GDPR. Any legal arguments put forward must also be grouped and referenced in relation to the operative part of the LSA's Draft Decision to which they relate.

Complainants' Rights

Under the current GDPR rules, the handling of complaints, as lodged by data subjects, also remains fragmented in cross-border cases. The Proposal seeks to harmonise this procedure, ensuring that complaints will be dealt with uniformly and regardless of where the complaint is lodged, or which national DPA is assigned as the LSA.

Complainants will also benefit from a bolstered right to be heard under the Proposal. In the event of a full or partial rejection of their complaint, complainants will have the opportunity to make their views known before the submission of a Draft Decision, or before a Revised Draft Decision (Article 12), or the issuing of a Binding

DATA PROTECTION

Decision. They may further request access to the non-confidential versions of documents that serve as the basis for the decision.

Finally, the Proposal accepts the use of amicable settlements between the controller and the data subject, but the relevant DPA may still conduct an *ex officio* investigation of the same controller if there is a suspected repeated or systemic infringement of the GDPR.

Key Takeaways

The Proposal seeks to improve GDPR enforcement proceedings through more cooperation and streamlined procedures. It pushes DPAs to find consensus and thereby seeks to limit the instances that differences between LSA and CSAs must be settled through the mechanism of binding decisions by the EDPB. Moreover, the Proposal establishes clearer rights for both parties under investigation and complainants.

European Commission Adopts Adequacy Decision for Transatlantic Transfers of Personal Data

On 10 July 2023, the European Commission (***Commission***) adopted an adequacy decision for the EU-US Data Privacy Framework (***DPF***). Under Chapter V of the General Data Protection Regulation (***GDPR***), transfers of personal data outside the European Economic Area (***EEA***) are prohibited (i) unless the intended destination jurisdiction(s) offer(s) an "*adequate level of protection*" of personal data when compared to that guaranteed pursuant to EU law (Article 45 GDPR; (ii) unless appropriate safeguards are put in place (Article 46 GDPR; or (iii) unless specific derogations apply (Article 49 GDPR.

Under EU law, an adequacy decision constitutes one of the key legal mechanisms for a transfer of personal data outside the EEA. Such a decision is a determination made by the Commission that a given jurisdiction, sector, or international organisation offers an adequate standard of protection of personal data. It allows for the unrestricted transfer of personal data from the EEA to the concerned entity.

The US had created two self-certification schemes that enjoyed adequacy status, but both were annulled: the Safe Harbor, which applied from 2000 until its invalidation by the Court of Justice of the European Union (***CJEU***) in 2015 (judgment of 6 October 2015, *Schrems I*), and – subsequently – the Privacy Shield, from 2016 until its invalidation in 2020 (judgment of 16 July 2020, *Schrems II*).

In *Schrems II*, the CJEU held that the limitations on the protection of personal data, resulting from US authorities' access to these data for national security and law enforcement purposes, as well as the prescribed remedies, were not defined in a manner that is "*essentially equivalent*" to those prevailing under EU law.

The DPF is supposed to remedy these shortcomings and to establish a satisfactory level of protection of personal data to individuals residing in the EEA.

What Are New Safeguards?

The adequacy decision – dated 10 July 2023 – entered into force on 11 July 2023, following a series of long, bilateral negotiations and the resulting changes in US surveillance law and practice. Most importantly, US President Biden's Executive Order 14086 of 7 October 2022 on "*Enhancing Safeguards for United States Signals Intelligence Activities*" and a Regulation on the Data Protection Review Court issued by the US Attorney General (14 October 2022 are intended to address the previous EEA data privacy concerns (raised especially in *Schrems II*).

One core element of the new safeguards is that, in accessing the personal data of EEA individuals, US authorities must conduct a balancing test to ensure that any access to the data is necessary and proportionate. US authorities will also be subject to greater oversight – by both judicial and non-judicial bodies, such as the Privacy and Civil Liberties Oversight Board (***PCLOB***), the Department of Justice (***DoJ***) and various committees of the US Congress – to ensure compliance with these rules.

DATA PROTECTION

A further novelty is the establishment of an independent and impartial redress mechanism. Under the DPF, EEA individuals can resolve their complaints before the so-called Data Protection Review Court (***DPRC***). An EEA individual wishing to lodge such a complaint must submit it to a relevant national Data Protection Authority (***DPA***) which will channel the complaint to the redress mechanism via the secretariat of the European Data Protection Board (***EDPB***).

How Does DPF Function?

The DPF is a self-certification mechanism which is open to US organisations that are subject to the jurisdiction of the Federal Trade Commission (***FTC***) or the Department of Transport (***DoT***). To benefit from the DPF, an American organisation receiving personal data from an EEA exporter must certify its participation in the DPF by completing and sending a self-certification submission to the Department of Commerce (***DoC***). Organisations must also pay an annual fee to utilise the DFP.

Once the DoC has determined that the initial self-certification is complete, the organisation will be placed on the public DPF List. From that moment, the organisation can rely on the adequacy decision to transfer personal data from the EEA to the US in compliance with Chapter V of the GDPR.

The DoC may remove an organisation from the list if that organisation voluntarily withdraws, fails to complete its annual re-certification, or persistently fails to comply with the DPF principles. Both the FTC and the DoT will monitor and enforce compliance with the DPF.

What Are Principles of DPF?

The principles which organisations must comply with are listed in Annex I to the adequacy decision and can be summarised as follows:

1. **Notice** – informing individuals about participation in the DPF, the purposes of the data collection, and of third parties that may have access to the data;
2. **Choice** – allowing individuals to choose whether their personal data may be disclosed to a third party;
3. **Accountability for Onward Transfers** – additional responsibilities for an organisation intending to forward personal data;
4. **Security** – commitment to taking "*reasonable and appropriate*" security measures to protect personal data;
5. **Data Integrity and Purpose Limitation** – generally limiting processing of personal data to the purpose for which it was collected, or closely related to that purpose;
6. **Access** – allowing individuals to access their personal data and make corrections or delete mistakes;
7. **Recourse, Enforcement, and Liability** – a baseline standard for potential recourse, including a "*readily available independent recourse mechanism*" or "*follow-up procedures*" to verify an organisation's compliance, and an "*obligation to remedy*" any violation of these principles.

How Does DPF Apply to Transfers from UK?

Following the withdrawal of the United Kingdom (***UK***) from the EU (Brexit), the UK retained – until its own reform of data protection law takes place – the GDPR and all adequacy decisions taken before Brexit.

However, the EU-US DPF – as concluded after 31 December 2020 – does not apply to the UK.

In turn, organisations in the UK wishing to transfer personal data to the US may benefit from the UK Extension to the DPF. Organisations must apply to the DoC to use this transfer mechanism.

DATA PROTECTION

Key Takeaways

Industry welcomed the new adequacy decision. In the short term, organisations can sign up to the principles which resemble those of the previous EU-US mechanism. They will have to maintain certification by informing data subjects of their rights under the DPF, aligning their privacy policies with the DPF and updating them regularly, and cooperating with DPAs when necessary. To facilitate this, both the Commission and the EDPB have already published Q&As.

In the longer term, the DPF, like its predecessors, is likely to be challenged before the CJEU. In parallel, the EC is obliged to periodically review all adequacy decisions (Article 45(3) GDPR) and the first such review is due before 10 July 2024.

Court of Justice of European Union Confirms Broad Scope of Right of Access Under General Data Protection Regulation

On 22 June 2023, the Court of Justice of the European Union (***CJEU***) delivered its judgment in *Pankki S* (C-579/21), which concerns the individual's right to access his or her personal data under Article 15 of the General Data Protection Regulation (***GDPR***).

Background

The case before the CJEU concerned an individual, J.M., who was both a customer and employee of the Finnish bank Pankki S. In 2014, J.M. discovered that his customer data had been accessed several times between 1 November and 31 December 2013 by Pankki S employees. Doubting the legality of those searches, J.M. – who was no longer an employee of the bank – requested the names of those who consulted his customer data, the exact dates of the consultations and the purposes for why his data was consulted.

In its reply, Pankki S refused to disclose the identity of the employees who accessed the information for privacy reasons, but it offered further details of the consultation operations.

J.M. applied to the Finish data protection authority (***DPA***) for an order that mandated Pankki S to provide him with the employee identities. On 4 August 2020, the DPA rejected J.M.'s application stating that log data constituted personal data of the employees who processed the data and not of the person whose data was accessed.

J.M. then brought an action against the DPA's decision in the Administrative Court of Eastern Finland (the ***Referring Court***). As the matter required interpretation of EU law, the Referring Court asked the CJEU for a preliminary ruling.

CJEU Judgment

How broad is the scope of the right of access? Does it extend to the name of the individuals who carried out the processing under instructions?

In its judgment, the CJEU first considered the purpose of the right of access. The CJEU observed that this right is key to ensuring the transparency of how one's personal data is processed, without which an individual would not be able to assess the legality of the processing of his or her data. Access is also necessary to exercise other rights conferred by the GDPR (e.g., the right to rectification of inaccurate personal data) or to seek remedies should the GDPR be infringed.

The CJEU further considered that a textual reading of the GDPR supports a broad interpretation of the right of access. In particular, the CJEU noted that "personal data" (Article 4(1) GDPR) is defined as "*any information relating to an identified/identifiable natural person*" and that an "*identified/identifiable natural person*" can be "*identified, directly or indirectly, by reference … or by one or more factors specific to a person*". The phrase "*any information*" encompasses all sorts of information, objective and subjective, whereby the contents, purpose or effect is connected to an identified or identifiable person. Therefore, the scope of "personal data" also includes all information resulting from the processing of personal data, such as log data, provided it relates to an identified or identifiable person.

DATA PROTECTION

The CJEU also noted that the employees acted under the authority of the bank and in accordance with its instructions. While the right of access encompasses a right to know the recipients of personal data (Article 15(1)(c) GDPR), the employees cannot be regarded as such recipients but rather as people processing personal data under the authority of the controller or processor (Article 29 GDPR).

Under what circumstances can meta-data containing personal data (such as log data) be disclosed to an individual pursuant to the right of access?

In the present case, J.M. received from Pankki S all the information which he was seeking, except for the names of the employees who consulted his personal data, which he argued was necessary for him to be able to check the lawfulness of the purposes communicated to him.

The CJEU observed that while the names of employees might fall under the scope of the right of access, they also constitute personal data under the GDPR. Necessarily, their interests need to be protected too. Recital 63 GDPR states that the right of access "*should not adversely affect the rights or freedoms of others*". Ultimately, knowing the employees' names might also infringe on their rights and freedoms.

The CJEU concluded that a balance must be struck between the rights of both individuals. If an individual believes the information provided by an organisation is not enough for his or her purposes, he or she has the right to lodge a complaint with a DPA.

Does it matter if the bank performed a regulated activity or that the individual is both a customer and client of the bank?

In reply, the CJEU noted that there is no provision in the GDPR that draws a distinction according to the nature of the activities of the organisation or the status of the person whose data was processed. While the GDPR allows EU Member States to limit the scope of obligations and rights under Article 15 GDPR, Finland had not subjected Pankki S's activities to such legislation.

The Court further explained that the status of the individual has no bearing on the scope of the right to access.

Does it matter whether the data was processed before the GDPR came into effect?

The CJEU noted that Article 15 GDPR grants a procedural right of obtaining information about the processing of personal data and that procedural rights generally only apply once a piece of legislation has come into effect. By contrast, substantive rules usually apply to situations that have arisen and become definitive after their entry into force.

As a result, since the rule at issue is a procedural rule, Article 15 GDPR applies to requests for access made after the GDPR came into effect, even if the data was processed before the regulation became applicable.

Takeaways

The judgment in *Pankki S* follows on the heels of other CJEU judgments concerning the right of access under Article 15 GDPR. For example, in a judgment of 4 May 2023, the CJEU held that individuals must be given a "faithful and intelligible" reproduction of their personal data. This judgment clarified that the right of access may require organisations to provide extracts of databases or even entire documents if they are essential for the effective exercise of the individual's rights under the GDPR (*See* our Client Alert of 11 May 2023).

The present case offers further clarification as to what information must be provided.

First, the most important aspect of this judgment is the scope of the right to access. While certainly broad, an organisation may leave out or redact information if required to protect the fundamental rights of other people.

DATA PROTECTION

Second, the individual has the right to request access to his or her personal data even if those data were processed before the GDPR came into operation on 25 May 2018. This may pose a burden in terms of cost and time for organisations with long-standing clients.

Third, the type of organisation and whether such an organisation acts within the framework of a regulated activity generally has no bearing on the scope of the right to access. The status of the person making the request is equally not relevant. This is important for clients who operate in a regulated industry that provide for an independent right of access, such as patient rights (cf. e.g., Article 5(d) of Directive on patients' rights in cross-border healthcare). These organisations may have to verify whether a request was made under the GDPR or other applicable rules.

Court of Justice of European Union Clarifies Legal Basis and Use of Sensitive Data for Personalised Advertising

Introduction

On 4 July 2023, the Court of Justice of the European Union (***CJEU***) gave judgment in *Meta Platforms Inc. and others v. Bundeskartellamt* (C-252/21) and shed light on two aspects of EU data protection law.

First, the judgment considers the interplay between EU competition law and data protection law. The question is whether competition authorities are permitted to analyse a firm's GDPR compliance (or non-compliance) when assessing an alleged abuse of dominant position and whether they can prohibit a dominant firm from engaging in specific data processing activities to bring an Article 102 TFEU infringement to an end.

Second, the judgment interprets specific provisions of the General Data Protection Regulation (***GDPR***), namely: the legal bases for processing personal data, making sensitive data manifestly public, and the validity of data subject's consent.

Both aspects were discussed in our recent client alert.

Background

In 2019, the *Bundeskartellamt*, the German competition regulator, found that Meta Platforms Inc. (***Meta***) had collected data from services affiliated with its social networking site Facebook (Instagram and WhatsApp), as well as third-party websites and applications, and linked these data with users' Facebook accounts without obtaining users' valid consent in accordance with the GDPR.

Although users authorised the linking of their personal data when clicking the sign-up button, the *Bundeskartellamt* found that users could not be considered to have given their consent 'freely', as required by the GDPR, considering Meta's dominant position and the fact that consent to data processing was a prerequisite for using Facebook. It concluded that this violation of GDPR rules constituted an (abusive) "*manifestation of Meta's market power*" and therefore infringed the EU competition law rules.

On appeal, the *Oberlandesgericht Düsseldorf* (Higher Regional Court) requested a preliminary ruling.

CJEU Judgment

When can an operator of a social network site rely on a contract as a legal basis for the processing of personal data for purposes such as personalised advertising or seamless functioning? Can it rely on a legitimate interest for such purposes?

The central question before the CJEU relates to the legal basis on which Meta relies to collect personal data of users of various services offered by the Meta group and the linking of such data with the data collected on Facebook. The *Bundeskartellamt* found that Meta had collected data from services affiliated with Facebook (e.g., Instagram and WhatsApp) as well as third-party websites and applications, and linked these data with users' Facebook accounts, without obtaining users' valid consent.

DATA PROTECTION

GDPR requires that any processing of personal data have a legal basis, such as the free consent of an individual or a legitimate interest of an organisation processing personal data.

The CJEU held that the processing of personal data pursuant to a contract to which a data subject is a party (Article 6(1)(b) GDPR) may justify the processing "*only on condition that the processing is objectively indispensable for a purpose that is integral to the contractual obligation intended for those users, such that the main subject matter of the contract cannot be achieved if that processing does not occur*" (para. 125). The CJEU added that the data controller must be able to demonstrate how the objective of the contract cannot be achieved if the processing in question does not occur. It specified that the processing of personal data will only be considered essential to the performance of the contract if there are no workable, less intrusive alternatives.

Furthermore, the CJEU ruled that personalised advertising by which an online social network finances its activity cannot justify, as a legitimate interest (Article 6(1)(f)), the processing of personal data in the absence of the data subject's consent. According to the CJEU, users would not expect that their personal data would be used for personalised advertising without their consent, and therefore, the interests of the data subject should prevail over Meta's legitimate interests. In particular, the CJEU considered that the collection of personal data for personalised advertising "*may give rise to the feeling that his or her private life is being continuously monitored*" (para. 118).

The CJEU also followed the Advocate General's Opinion that when the contract consists of several separate services or elements of a service that can be performed independently of one another, the applicability of that rule should be assessed for each of those services separately (para.100; AG Opinion, para. 54).

In what circumstances does a user of a social network site make his or her 'sensitive' personal data manifestly public?

The GDPR affords special protection to the so-called special categories of personal data which may reveal, *inter alia*, racial or ethnic origin, political opinions, religious beliefs or sexual orientation ('sensitive' data - Article 9(1)). The processing of such 'sensitive' data is normally prohibited unless a derogation applies. In the case at hand, it was established that Meta processes sensitive data when it collects personal data from users of the social network Facebook "*when they visit websites or apps*" or "*when they register or place online orders*" (para. 71) (which can be linked to the data of other users' social network accounts). The information collected in this manner may reveal or create 'sensitive' categories of personal data.

Meta argued that the individual made his or her own 'sensitive' data manifestly public which gave Meta a valid reason to process those data under Article 9(2)(e). The CJEU observed that for this derogation to apply an individual must intend, "*explicitly and by a clear affirmative action, to make the personal data* [...] *accessible to the general public*" (para. 77). Consequently, the CJEU clarified that the mere fact that a user of an online social network visits websites or uses applications that may reveal their 'sensitive' data **does not** imply that the individual manifestly makes such data public (para. 84) and therefore Meta cannot rely on Article 9(2)(e) GDPR for the information it collected in this manner.

By contrast, when the user "*enters information into such websites or apps*", "*clicks or taps on buttons integrated into those sites and apps, such as the 'Like' or 'Share' buttons*" or clicks or taps on "*buttons enabling the user to identify* [...] *on those sites or apps*", that user does manifestly make public the data thus entered, but "*only* [when] *he or she has explicitly made the choice beforehand*" to make such data public, including making them available "*to an unlimited number of persons*", and "*on the basis of individual settings selected with full knowledge of the facts*" (para. 85; emphasis ours). In these cases, Meta would be allowed to rely on the derogation provided for by Article 9(2)(e) GDPR.

DATA PROTECTION

Does the fact that an organisation holds a dominant position on the market impact the validity of the individual's consent to process personal data by that organisation?

Under the GPDR, the individual's consent as a legal basis for processing personal data (Article 6(1)(a)) GDPR is valid only if it is "*freely given, specific, informed and unambiguous*" (Article 4(11

The CJEU held that "*the fact that the operator of an online social network holds a dominant position on the market for online social networks does not, as such, preclude the users of such a network from being able validly to consent* [...] *to the processing of their personal data by that operator*" (para. 154. However, the CJEU added that the dominant position is important "*in determining whether the consent was in fact validly and, in particular, freely given, which it is for that operator to prove*" (para. 154).

Key Takeaways

The CJEU established a high burden for organisations that seek to justify processing for the purposes of personalised advertisements on contractual grounds or, alternatively, the legitimate interest pursued by the data controller.

The CJEU further clarified that the mere visiting of websites does not make the 'sensitive' personal data manifestly public, as doing so requires the explicit and "*clear affirmative action*" of the data subject.

Finally, the CJEU held that having a dominant position does not, as such, stand in the way of the individual consent to be given freely and validly. Still, that dominant position will be a factor in the analysis.

INTELLECTUAL PROPERTY

European Union Intellectual Property Office Publishes New Report on Litigation Trends Regarding Trade Secrets

On 28 June 2023, the European Union Intellectual Property Office (***EUIPO***) published a new report on litigation trends regarding the unlawful acquisition, use or disclosure of trade secrets, as required by Article 18 of Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (the ***Report***). The Report focuses on trade secrets litigation between 1 January 2017 and 31 October 2022.

Quantitative Analysis

The Report contains a quantitative analysis of trade secret litigation. It found that in 27% of cases the courts confirmed the infringement of the trade secret. However, this percentage varies significantly among Member States, with some jurisdictions reporting confirmation rates as high as 41%. The Report also found that trade secret litigation still presents a differing picture across Member States on a range of issues such as case volumes, case types, legal forums, procedure. Interestingly, the Report emphasises that trade secret disputes predominantly occur at the national level, making cross-border trade secrets litigation a relatively uncommon occurrence.

Qualitative Analysis

The Report also delves into qualitative aspects of trade secret litigation in the EU. Notable trends in that regard include the existence of more flexible interpretations of the "reasonable steps" outlined in Article 2(1 of Directive 2016/943 and the importance of explicitly identifying trade secrets in contracts in order to meet the criterion for trade secret protection. Moreover, the Report shows that trade secret holders still face challenges in safeguarding the confidentiality of their trade secrets in the course of legal proceedings. Concerns about unintended disclosure persist, leading to a tendency for valid infringement claims to be dismissed due to insufficient clarity and specificity in these cases.

Belgium

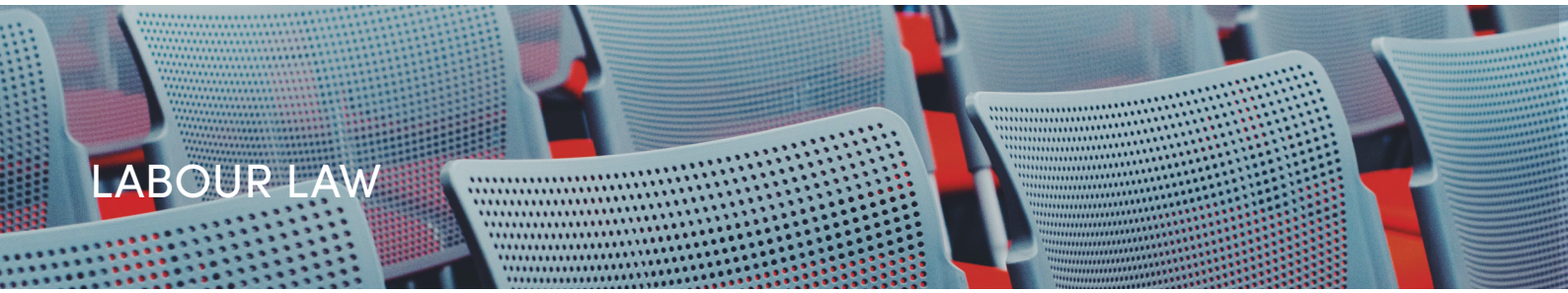
The Report mentions 59 trade secrets proceedings in Belgium. 16% of the cases were appealed. One out of three infringement proceedings were successful. All reported cases qualify as civil cases and the claimants were mostly private businesses. In one out of three cases, the defendant was a former employee of the claimant. As a result, some of the cases were brought before a specialised labour court. Other cases were handled by the regional commercial courts. The low appeal rate and the fact that the cases are handled by regional commercial courts is in contrast with other jurisdictions in the EU.

The majority of the cases concerned breaches of confidentiality agreements (36%); unauthorised acquisition to trade secrets based on direct unauthorised access (21%); and unauthorised use or disclosure based on unauthorised acquisition (23%).

The most commonly raised defence, and that with the highest success rate, is that no trade secret exists because the information is generally known and is not secret. There were 19 concurrent claims of unfair competition within the same proceedings; in these instances, the unfair competition claim was successful on 8 occasions (42 % success rate).

As regards enforcement, in most proceedings (80%) the court issued an injunctive measure of cessation and prohibition to use the trade secret.

The Report is available here.



LABOUR LAW

New Provisions Governing Incapacity For Work During Holidays Require Adjustments To Work Rules

On 31 July 2023, the Law of 17 July 2023 amending the Law of 3 July 1978 on employment contracts and the Law of 8 April 1965 establishing work rules relating to the concurrence of annual leave and incapacity for work was published in the Belgian Official Journal (*Wet van 17 juli 2023 tot wijziging van de Wet van 3 juli 1978 betreffende de arbeidsovereenkomsten en de Wet van 8 april 1965 tot instelling van de arbeidsreglementen met betrekking tot de samenloop van jaarlijkse vakantie en arbeidsongeschiktheid / Loi du 17 juillet 2023 modifiant la loi du 3 juillet 1978 relative aux contrats de travail et la loi du 8 avril 1965 instituant les règlements de travail en ce qui concerne la coïncidence des vacances annuelles et de l'incapacité de travail* – the ***Law***). The Law provides for a legal framework to address the recent modifications made to the Royal Decree of 30 March 1967 which was amended to comply with Directive 2003/88/EC of 4 November 2003 concerning certain aspects of the organisation of working time (the ***European Working Time Directive***) (*Koninklijk Besluit van 30 maart 1967 tot bepaling van de algemene uitvoeringsmodaliteiten van de wetten betreffende de jaarlijkse vakantie van de werknemers / Arrêté royal portant modification des articles 3, 35, 46, 60, 64, 66 et 68 et insérant un article 67bis dans l'arrêté royal du 30 mars 1967 déterminant les modalités générales d'exécution des lois relatives aux vacances annuelles des travailleurs salaries* – the ***Vacation Rules***).

Changes to Vacation Rules

To implement the European Working Time Directive, the Vacation Rules were amended to guarantee that employees consistently have the right to a minimum of four weeks of paid vacation. One of these measures allows employees who are unable to work during their scheduled holidays to have those days converted into sick leave (*See*, this Newsletter, Volume 2023, No. 3).

Labour Law Framework

As of 2024, the following rules will apply if the employee wishes his holidays to be converted into sick leave:

- The employee is required to inform the employer promptly regarding his incapacity for work during his holidays and provide his residential address if that is different from his home address.
- The employee is required to provide the employer with a medical certificate within two working days from either the start of incapacity or the receipt of the employer's request. This timeline may be adjusted if stipulated differently in a collective bargaining agreement or the work rules. Under unforeseen circumstances, the employee should provide the medical certificate within a reasonable timeframe.
- The medical certificate should specify the work incapacity, its probable duration, and whether or not the employee is permitted to travel.
- When presenting the medical certificate, the employee must explicitly inform the employer of his intention to defer and maintain the vacation days that coincide with his work incapacity.

Starting 1 January 2024, it is mandatory for all employers to incorporate in the work rules the terms that should be followed in cases of illness-related work incapacity during a period of holidays. However, these terms can be incorporated by a simplified procedure: there is no need to consult staff. By contrast, the revised work rules must still be presented to the Social Inspectorate.

The Law can be found here (Dutch) and here (French).

Brussels
Glaverbel Building
Chaussée de La Hulpe 166
Terhulpsesteenweg
B-1170 Brussels
Belgium

Phone:+32 (0)2 647 73 50
Fax:+32 (0)2 640 64 99

Geneva
26, Bd des Philosophes
CH-1205 Geneva
Switzerland

Phone:+41 (0)22 320 90 20
Fax:+41 (0)22 320 94 20

London
Holborn Gate
330 High Holborn
London
WC1V 7QH
United Kingdom

Phone: +44 (0)20 7406 1471

VAN BAEL & BELLIS

www.vbb.com