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

Legal 500 2019

January 2022

VBB on Belgian Business Law

Highlights

"Van Bael & Bellis excels in M&A work, and often provides domestic Belgian law advice on cross-border transactions."

IFLR1000, 2019

Topics covered in this issue

Van Bael & Bellis on Belgian Business Law should not be construed as legal advice on any specific facts or circumstances. The content is intended for general informational purposes only. Readers should consult attorneys at the firm concerning any specific legal questions or the relevance of the subjects discussed herein to particular factual circumstances.

vbb@vbb.com
www.vbb.com

Table of contents

Van Bael & Bellis on Belgian Business Law should not be construed as legal advice on any specific facts or circumstances. The content is intended for general informational purposes only. Readers should consult attorneys at the firm concerning any specific legal questions or the relevance of the subjects discussed herein to particular factual circumstances.

© 2022 Van Bael & Bellis

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

Phone: +32 (0)2 647 73 50 vbb@vbb.com
Fax: +32 (0)2 640 64 99 www.vbb.com

COMMERCIAL LAW

Federal Parliament Increases Protection of Commercial Agents

On 3 February 2022, the federal Chamber of Representatives adopted a Law modifying the Code of Economic Law with respect to commercial agency agreements with a view of protecting commercial agents against unilateral increases of expenses or their imposition by the principal (*Wet tot wijziging van het Wetboek van Economisch Recht inzake de handelsagentuurovereenkomsten houdende de bescherming van handelsagenten tegen de eenzijdige verhoging of oplegging van de kosten door de principaal / Loi modifiant le Code de droit économique en ce qui concerne les contrats d'agence commerciale en vue de prémunir les agents commerciaux contre l'augmentation unilatérale des frais ou leur imposition par le commettant* - the ***Law***).

A private member's Bill was first presented to the Chamber of Representatives on 6 July 2021 in an attempt to address concerns voiced by BZB-Fedafin, the largest professional organisation of self-employed commercial agents, regarding the supposedly insufficient protection of self-employed commercial agents *vis-à-vis* their principals.

Commissions

By way of background, commercial agents are frequently bound to their principals by exclusivity clauses and non-compete obligations. A commercial agent terminating a contract with its principal will generally lose the right to an indemnity and, due to the non-compete obligation, will not be able to work for another principal for a period of time – generally six months.

The existing regulatory framework applicable to commercial agents considers a unilateral attempt to modify the agent's initially agreed commissions (*commissies / commissions*) as a form of constructive termination of the commercial agency agreement (*handeling die gelijkstaat met verbreking / acte équipollent à rupture*). Commercial agents who rely on this provision may claim an indemnity in relation to such constructive termination. Additionally, they do not fall under the non-compete contained in the agreement and may thus start working for another principal. A court may nonetheless find that an agent who unreservedly accepted reduced commissions for a relatively long period of time tacitly agreed to this modification (*See,* Article X.13, seventh indent of the Code of Economic Law; the ***CEL***).

Expenses

However, this regulatory framework was considered to be insufficiently protective of independent commercial agents. In particular, before the Committee for the Economy, Consumer Protection and the Digital Agenda of the federal Chamber of Representatives it was explained that principals in the financial sector frequently increase expenses incumbent on commercial agents in circumvention of Article X.13 CEL. These expenses relate to matters such as cash transaction fees, the maintenance of automatic teller machines (ATMs), marketing, contributions to specific taxes, and fees for legal services.

This is why the Law added a new paragraph to Article X.13 CEL which provides that, although the parties to a commercial agency agreement may freely establish the expenses incumbent on the agent, any unilateral attempt to substantially or structurally increase or impose expenses will be construed as a constructive termination of the agreement. However, mirroring the existing regime governing unilateral modifications to an agent's commissions, the new paragraph also empowers a court to find that a commercial agent who unreservedly accepted such an increase or imposition for a relatively long period of time tacitly agreed to the change.

© 2022 Van Bael & Bellis

Court of Justice of European Union Holds That National Courts Are Not Required to Disapply Domestic Provisions Contrary to EU Directive in Dispute Between Private Parties

On 18 January 2022, the Court of Justice of the European Union (***CJEU***), sitting in Grand Chamber, delivered a judgment concerning the issue of whether, in an action brought by a private individual against another private individual, a national court must disapply the provision of national law on which the action is based if that provision is contrary to an EU Directive (Case C-261/20, *Thelen Technopark Berlin*). The judgment provides insight into the relationship between national law and EU law when a national court is unable to interpret a national law in conformity with an EU Directive.

The Grand Chamber's judgment stems from a request for a preliminary ruling by the German Federal Court of Justice (*Bundesgerichtshof*) in proceedings between Thelen, a real estate company, and MN, an engineer. In 2016, the parties concluded a services agreement pursuant to which MN would perform several services for a flat fee of EUR 55,025. These services were covered by a 2013 German Decree on fees for services provided by architects and engineers, called the *Verordnung über die Honorare für Architekten- und Ingenieurleistungen (Honorarordnung für Architekten und Ingenieure* - the ***HOAI***). The HOAI essentially sets out minimum rates for services provided by architects and engineers. Upon termination of the agreement a year later, MN invoiced Thelen according to HOAI and, after payments already made, brought an action for EUR 102,935, which was more than the agreed upon contract price.

Following setbacks at the first and second instances, Thelen brought an appeal on points of law before the German Federal Court of Justice, which in turn submitted a request for a preliminary ruling to the CJEU. The Federal Court of Justice pointed out that in 2019 the CJEU held the HOAI to be incompatible with Article 15 of Directive 2006/123 of 12 December 2006 on services in the internal market (the ***Services Directive***), which prohibits Member States from maintaining requirements that make the exercise of a service activity subject to compliance by the provider with fixed minimum and/or maximum rates, if those requirements do not satisfy the cumulative conditions of non-discrimination, necessity and proportionality (Case C-377/17, *Commission v. Germany*). Additionally, just a year earlier, the CJEU had held that Article 15 of the Services Directive was sufficiently precise, clear and unconditional to be capable of having a direct effect (Joined Cases C-360/15 and C-31/16, *X and Visser*).

Against that background, the Federal Court of Justice asked the CJEU to determine whether, in a dispute between private parties, Article 15 of the Services Directive has direct effect in such a way that relevant provisions of the HOAI are invalid and should no longer be applied. However, if Article 15 of the Services Directive does not have such an effect, the Federal Court of Justice asked whether relevant provisions of the HOAI should then be considered contrary to EU law and thus no longer be applied in a dispute between private persons.

The principle of primacy of EU law normally requires all Member State bodies to give full effect to EU provisions. At the same time, the Grand Chamber recognised the existence of limits to this general principle. In particular, the Grand Chamber considered the nature and legal effects of EU Directives. A Directive is only intended to impose obligations on EU Member States and does not impose obligations on an individual. It therefore cannot be relied on against that individual before a national court. As a result, the Grand Chamber found that even a clear, precise and unconditional provision of a Directive does not allow a national court to disapply a conflicting national legal provision if this would have the effect of imposing an additional obligation on an individual. In doing so, the Grand Chamber refused to attribute to Article 15 of the Services Directive a "horizontal" direct effect, that is the possibility of being invoked in proceedings between private parties.

The Grand Chamber reasoned that if Article 15 of the Services Directive were to be applied in the main proceedings, MN would be deprived of the right to claim the rates referred to in the HOAI and would be forced to accept payment of the contractually agreed rates. Therefore, it found, the Federal Court of Justice was not required, in the context of a dispute between private parties and at least solely on the basis of EU law, to disapply the HOAI even if the latter is contrary to the Services Directive.

© 2022 Van Bael & Bellis

That said, pursuant to Article 260(1) of the Treaty on the Functioning of the European Union (***TFEU***), if a Member State was found by the CJEU to have breached an obligation under EU law, that Member State is required to take the necessary measures to comply with the judgment. Although the purpose of judgments handed down pursuant to Article 260 TFEU is to create obligations for Member States when they fail to abide by their obligations rather than confer rights on private individuals, a private party who has been harmed as a result of national law not being in conformity with EU law may obtain compensation for the loss or damage sustained as a result. To this end, three conditions must be satisfied: (i) the rule of EU law infringed upon must be intended to confer rights on individuals; (ii) the breach of that rule must be sufficiently serious; and (iii) there must be a direct causal link between that breach and the loss or damage sustained by that individual. With regard to the second condition, the Grand Chamber considered that a breach of EU law is clearly sufficiently serious if it has persisted despite a judgment finding the breach to be established. As a result, by maintaining fixed rates under the HOAI, Germany had committed a sufficiently serious breach of its obligations under Article 15 of the Services Directive.

On this basis, the Grand Chamber found that a national court is not required in a dispute between private individuals and solely on the basis of EU law to disapply a piece of national legislation that is in breach of an EU Directive. However, this finding is without prejudice to that national court's power to disapply the piece of legislation on the basis of domestic law and to the possibility for a private party who was harmed as a result of national law not being in conformity with EU law to claim compensation from the Member State for the resulting loss or damage.

© 2022 Van Bael & Bellis

COMPETITION LAW

Federal Parliament Adopts Bill Transposing ECN+ Directive and Reforming Belgian Competition Rules

On 21 December 2021, the federal government submitted to the Chamber of Representatives of the federal Parliament bill 55K2388 (the ***Bill***), which will modify the Belgian competition rules and also implement Directive 2019/1 of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market (the ***ECN+ Directive***) (*Wetsontwerp tot omzetting van Richtlijn (EU) nr. 2019/1 van het Europees Parlement en de Raad van 11 december 2018 tot toekenning van bevoegdheden aan de mededingingsautoriteiten van de lidstaten voor een doeltreffendere handhaving en ter waarborging van de goede werking van de interne markt / Projet de loi transposant la directive (UE) 2019/1 du Parlement européen et du Conseil du 11 décembre 2018 visant à doter les autorités de concurrence des Etats membres des moyens de mettre en oeuvre plus efficacement les règles de concurrence et à garantir le bon fonctionnement du marché intérieur*). The Bill had already been approved by the federal Council of Ministers in May 2021 (*See*, this Newsletter, Volume 2021, No 5). On 16 February 2022, an amended version of the initial text was adopted in second reading by the parliamentary Committee of Economic Affairs, Consumer Protection and Digital Agenda. The Bill was finally and unanimously adopted in plenary session on 24 February 2022.

The Bill comes over a year late, as the ECN+ Directive had to be implemented by 4 February 2021. The ECN+ Directive obliges Member States to ensure that national competition authorities have the means to apply Articles 101 and 102 TFEU more effectively. The ECN+ Directive requires that national competition authorities (i) be independent in enforcing competition law; (ii) have sufficient resources to carry out their work; (iii) have effective investigative tools to detect and bring competition law infringements to an end; (iv) have the ability to impose effective and dissuasive sanctions; (v) establish strong leniency programmes to detect cartels; and (vi) set up mechanisms for mutual assistance between competition authorities throughout the EU. In order to meet these objectives, the Bill amends a series of provisions of the Code of Economic Law (*Wetboek van Economisch Recht / Code de droit économique* – the ***CEL***).

However, the changes brought about by the Bill go beyond the implementation of the ECN+ Directive. The Bill covers a range of important subjects such as the organisation, functioning and powers of the Belgian Competition Authority (*Belgische Mededingingsautoriteit / Autorité belge de la Concurrence* – the ***BCA***), evidence, leniency applications, investigations, fines, and merger control. The main changes brought about by the Bill (as adopted on 16 February 2022) are described below.

Amendments to notions used in Belgian competition law

Article 3 of the Bill harmonises several competition law concepts. Two changes must be pointed out:

- The notion of "practice that restricts competition" (*restrictieve mededingingspraktijk / pratique restrictive de concurrence*) is replaced with the notion of "competition law infringement" (*inbreuk op het mededingingsrecht / infraction au droit de la concurrence*) in order to bring this notion in line with the concept used in Book XVII, title 3 CEL regarding damage actions following competition law infringements.

- The Bill clarifies that a "cartel" also includes horizontal agreements with a vertical component, such as "hub and spoke" infringements. This indirectly confirms that participants in such an infringement can seek leniency, which is in line with the practice of the BCA.

Financial Contributions to Merger Control Procedures

First, as announced in October 2021 by Minister of Economic Affairs Pierre-Yves Dermagne (*See*, this Newsletter, Volume 2021, No. 10), Article 6 of the Bill requires firms that notify a concentration to pay a fee which will amount to EUR 17,450 for mergers reviewed under the simplified procedure and to EUR 52,350 for mergers subject to the regular merger control procedure. These amounts will be indexed from 2023 based on the consumer price index. They can be amended by Royal Decree.

© 2022 Van Bael & Bellis

The commentary on the Bill explains that these amounts are meant to compensate the BCA for its merger control work and to strengthen the independence of the BCA. Merger notification fees already exist in other countries, including Denmark, Lithuania, the Netherlands, Romania, Switzerland and the United States.

Independence of the BCA

The Bill implements the ECN+ Directive by including in the CEL a general principle of operational independence of the BCA but specifies that this independence will not be compromised by the cooperation with other national competition authorities (***NCAs***) within the European Competition Network, nor by the BCA's obligation to be accountable, in particular through (i) the publication of its annual report which should be transmitted to the Chamber of Representatives; (ii) the judicial control carried out by the Markets Court (*Marktenhof / Cour des marchés*); as well as (iii) the control of the BCA's accounts and expenditure carried out by the Court of Auditors (Article 7 of the Bill). By contrast, Article 7 makes it clear that the BCA should not take orders from a government or from other entities, both public and private.

The regime of incompatibilities applicable to the BCA is also amended. Article 13 of the Bill provides that BCA officials must not deal with proceedings concerning undertakings for which they have worked or in which they have held office one year prior to their appointment to the BCA. Remarkably, this period is currently three years. While this change would not seem to contribute to the enhanced autonomy of the BCA, it is justified in the commentary on the Bill by an apparent need to follow the example of other Belgian regulators and by the wish that the BCA should "*benefit from the know-how acquired during a previous professional experience*".

Similarly, former BCA staff members must refrain, for a "*reasonable period of time*", from dealing with pending competition law proceedings that could give rise to conflicts of interest. For instance, former BCA officials must not be involved in a case on which they worked while at the BCA (Article 14 of the Bill).

Investigative Powers and Decisions of the BCA

Article 15 of the Bill clarifies that the right of the BCA to request information includes any information to which companies or individuals have access, not only information already in their possession. This makes clear that information stored in the cloud or on servers is concerned to the extent that companies have access to it. Any information can be requested, regardless of its form or medium. This includes electronic messages and instant messages.

The Bill also codifies the BCA's current practice in requiring the BCA to consult market participants formally or informally when it considers making commitments binding (Articles 26 to 28 and Article 32 of the Bill). The BCA can also convene to a hearing companies or individuals who may have information relevant to an investigation (Article 16 of the Bill). The Bill enables the BCA to impose a fine if a party refuses to attend a hearing (Article 69 of the Bill).

With respect to inspections, Article 17 of the Bill provides that the BCA can request the police force as a preventive measure during inspections. The BCA can also challenge the refusal of a judge to authorise an inspection before the Chamber of Indictments of the Brussels Court of Appeal (*Kamer van inbeschuldigingstelling / Chambre des mises en accusation*).

The same provision enables the BCA to record answers given by firms to its investigators. These answers can either be taken in writing or recorded on an electronic medium. If they are recorded, the interviewed person must receive a copy of the recording or a transcript of the answers in the form of inspection minutes (*proces-verbaal / procès-verbal*).

The duty of the public authorities and administrations to cooperate with a BCA investigation has been strengthened (Article 18 of the Bill).

The Bill also allows the BCA to end an *ex officio* investigation due to a lack of available resources or if the case is not considered to be a priority, *e.g.*, if the company concerned goes bankrupt; this is currently only possible for investigations following complaints and injunctions (Article 27 of the Bill).

© 2022 Van Bael & Bellis

Moreover, the Bill clarifies that, unless the CEL provides otherwise, all notifications and communications concerning a case will be made by e-mail with acknowledgment of receipt. Sending a copy by post will therefore no longer be necessary (Article 56 of the Bill).

Admissibility of Evidence Before the BCA

Article 21 of the Bill specifies the type of evidence that is admissible in proceedings before the BCA, including secret recordings made by companies or individuals that are not public authorities, provided that these recordings are not the sole source of evidence relied on by the BCA. Electronic messages, including unread or deleted messages, also qualify as admissible evidence. The commentary on the Bill confirms the application of the *Antigoon/Antigone* case law to competition law investigations (Supreme Court judgment of 14 October 2003). As a result, even illegally obtained information can be used as evidence by the BCA, except in the specific circumstances caught by this case law and reproduced in the Bill.

Article 22 of the Bill clarifies that it is incumbent on the firms or persons concerned to indicate to the BCA that some of the information provided (*e.g.*, following requests for information) or obtained (*e.g.*, in the context of inspections) should be treated as confidential. If no non-confidential version is submitted, the documents concerned will be deemed not to include confidential information. The companies or individuals concerned must indicate to the BCA that some information is confidential within ten days following the day on which the BCA obtained the information. At their request, the BCA can grant at least two months (which can be extended) to provide non-confidential versions. The BCA may also itself produce a non-confidential version of specific documents if it considers this to be in the interest of its investigation.

The Bill also establishes a new procedure known as the "ring agreement" which drew inspiration from the practice of the European Commission. This is a negotiated disclosure procedure through which a restricted circle of individuals is given access to confidential information contained in the instruction file. This procedure is intended to reduce the burden of preparing non-confidential versions of documents, especially when the file is voluminous.

Decisions and Fining Powers of the BCA

Article 34 of the Bill explicitly provides that the decisions of the BCA must be formally and adequately reasoned. This is assessed by reference to the criteria of the Law of 29 July 1991 regarding the formal reasoning in administrative decisions (*Wet betreffende de uitdrukkelijke motivering van de bestuurshandelingen / Loi relative à la motivation formelle des actes administratifs*), which the Markets Court has found to apply to the decisions of the BCA.

Additionally, while the current version of the CEL refers to an existing competition law infringement, Article 34 of the Bill empowers the BCA to find that an infringement has been committed in the past and to impose a fine for that infringement.

Article 66 of the Bill specifies that the BCA can impose a fine if an infringement of competition law was committed deliberately or negligently. The terms "deliberately or negligently" are meant to follow the case law of the EU Courts which holds that these concepts refer to situations in which the firm at issue cannot have been unaware of the anti-competitive nature of its conduct.

The same provision of the Bill also codifies the current practice of the BCA by explicitly requiring the BCA to "*take into account the gravity of the competition law infringement and its duration*" while imposing a fine.

Finally, the Bill completes the range of tools available to the BCA to sanction companies:

- While the current version of the CEL makes a breach of interim measures only subject to periodic penalty payments, the Bill now adds the possibility of imposing fines (Article 68).

- Conversely, in addition to the existing possibility to impose fines for procedural infringements of competition law, the Bill now empowers the BCA to impose periodic penalty payments for such infringements (Article 69).

© 2022 Van Bael & Bellis

- Similarly, in addition to the existing possibility to fine companies that implement a concentration before securing clearance from the BCA, the Bill now enables the BCA to fine companies that fail to notify a merger before implementing it. This second possibility existed in the 2013 version of the CEL but was removed in 2019. However, the EU Courts held in the meantime that this double sanctioning mechanism of gun-jumping conduct is not contrary to the *ne bis in idem* principle, which is why it is now reintroduced in Belgian law (Article 69).

Leniency and Immunity Applications

The Bill creates a new sub-section in the CEL which provides for the rules on leniency. Some of these rules are a codification of provisions that currently form part of guidelines (Articles 35 and following). Article 40 of the Bill clarifies that individuals can join their immunity application to the leniency application of a company (or trade association). In that case, individuals can obtain immunity if the company's application satisfies the conditions to obtain total or partial immunity from fines and if the individual actively cooperates with the BCA.

In Belgium, infringements of the rules governing public procurement can give rise not only to administrative fines (imposed by the BCA) but also to criminal sanctions (imposed by the criminal courts). This may deter these persons from seeking leniency with the BCA. This is why Article 76 of the Bill amends Article 314 of the Criminal Code to enable public prosecutors (*openbaar ministerie / ministère public*) to grant full or partial immunity from criminal sanctions to individuals involved in bid rigging, if these individuals cooperate with the public prosecutors and if they also applied for immunity with the BCA.

Settlements

In line with the Royal Decree of 30 August 2013 on the procedure for the protection of competition (*Koninklijk Besluit betreffende de procedures inzake bescherming van de mededinging / Arrêté Royal relatif aux procédures en matière de protection de la concurrence*), the Bill provides for a time period of at least two weeks within which the parties may indicate in writing that they are willing to enter into settlement discussions with the BCA or voluntarily file a settlement statement (Articles 43 and 45 of the Bill).

Interim Measures

Article 55 of the Bill enables the Competition Prosecutors (*Auditoraat / Auditorat*) of the BCA to file written observations regarding the interim measures which the Competition College (*Mededingingscollege / Collège de la Concurrence*) considers imposing on companies or trade associations.

Cooperation Between National Competition Authorities

The BCA, other NCAs and the European Commission cooperate via information and consultation mechanisms described in Articles 58 to 65. Under certain circumstances, the BCA can share a leniency application with other NCAs and with the European Commission (Article 59 of the Bill).

At the request of another NCA, the BCA can notify a company, trade association or individual of a procedural act or decision taken by this NCA pursuant to Articles 101 and 102 TFEU (Article 61 of the Bill). The BCA can request the same service from another NCA (Article 62 of the Bill).

Similarly, the BCA can execute decisions imposing fines and penalty payments adopted by other NCAs under specific conditions (Article 63 of the Bill), and, conversely, request another NCA to execute its own decisions (Article 64 of the Bill).

Both mechanisms rely on the use of a "uniform instrument" (*uniform instrument / instrument uniforme*) described in Article 65 of the Bill, to which a copy of the act or decision to notify or execute is attached.

Powers of the Markets Court

Finally, Article 73 of the Bill empowers the Markets Court to hear appeals relating to the legality of notifications made by the BCA of acts and decisions of other NCAs and execution by the BCA of decisions of other NCAs, as well as the legality of requests by the BCA to have its acts or decisions notified or executed by other NCAs (as set out under Articles 61 to 64 of the Bill).

© 2022 Van Bael & Bellis

Additionally, as the amount of the merger control fee introduced by the Bill will depend on whether the merger is reviewed under the simplified procedure or the regular merger control procedure, Article 73 of the Bill introduces the possibility for the firms concerned to challenge a decision by which the BCA rejects the application of the simplified procedure.

Belgian Competition Authority Gives Green Light for Port of Antwerp-Bruges Merger

On 7 January 2022, the Belgian Competition Authority (*Belgische Mededingingsautoriteit / Autorité belge de la Concurrence* - ***BCA***) unconditionally cleared the merger of the Port of Antwerp and the Port of Zeebrugge. The merged entity will operate under the name "Port of Antwerp-Bruges". The Port of Antwerp-Bruges will become the largest container port, and the second largest port overall, in Europe. The merger follows a trend towards increasing concentration in the European ports landscape already observed in France, Italy and Spain.

The parties justified their merger by the complementary nature of the ports of Antwerp and Zeebrugge, each having different product portfolios. For instance, the Port of Antwerp houses the world's second largest chemical cluster after Houston. The Port of Zeebrugge, on the other hand, is one of the biggest car ports in the world and has a large LNG (liquified natural gas) terminal. The parties expressed the wish to jointly tackle shared challenges such as the significant consolidation of the downstream market (which enables both terminal operators and shipping lines to exert price pressure on the merged entity and leads to increased competition between ports for cargo), market demand for economies of scale and optimisation of the logistics chain, and recent developments in the fields of energy transition and digitalisation.

In its assessment, the BCA did not define the relevant product markets. The BCA did not rule out that all ports might compete with each other, irrespective of their differences. Each port has its own blend of economic activities, such as the offer of port concessions (*i.e.*, the renting of space to companies that carry out port-related activities) and the provision of general port services (*i.e.*, services which entail granting access to the port and making the port infrastructure available in exchange for a fee) and special port services (which include smaller services such as towage, pilotage, mooring and unmooring and the supply of drinking water and electricity in return for a fee). This mix of activities allows each port to determine its activities in order to adjust to the competition of other ports.

The BCA considered the following markets to be affected by the transaction:

- The offer of port concessions for containers;
- General port services for containers;
- The offer of port concessions for liquid bulk;
- General port services for liquid bulk;
- The offer of port concessions for roll-on/roll-off cargo ("ro-ro cargo"); and
- General port services for ro-ro cargo.

The BCA found the geographical market for the provision of port concessions for containers and liquid bulk and general port services for containers and liquid bulk to be the so-called "*Hamburg-Le Havre*" (HLH) range, which is composed of nine ports between Hamburg and Le Havre. Concerning port concessions for ro-ro cargo and general port services for ro-ro cargo, the BCA found the geographical market to be limited to the Rotterdam-Dunkerque range.

Regarding special port services, the BCA found that these services "*may be port-specific*", which means that there cannot be any horizontal overlap between the services provided at each port and therefore no affected market. However, the BCA also indicated that "*if pricing and/or quality are considered as possible competition parameters, the HLH range is the relevant geographic market*". The BCA concluded that, since a breakdown by cargo type was "*not relevant*" for special port services, the relative position of the parties and their competitors on this market could be estimated based on overall market shares. As a result, the market share of the parties for special port services was below 25% and the market was therefore not affected by the merger.

© 2022 Van Bael & Bellis

The BCA did not identify competition issues on any of the affected markets. The BCA found that the transaction did not lead to such a significant change of market structure that the existence of coordinated effects should be examined. Additionally, the BCA considered that the non-coordinated horizontal effects brought about by the merger would not result in effective competition being significantly impeded on the markets for the provision of port concessions and for general port services for containers, liquid bulk and ro-ro cargo.

The BCA concluded that the merger could be cleared without conditions. The integration of both ports is planned to be finalised within one year.

Federal Council of Ministers Appoints New Competition College of Belgian Competition Authority

On 4 February 2022, the Federal Council of Ministers (*Ministerraad / Conseil des Ministres*) approved a draft Royal Decree that will appoint 16 members (*Assessoren / Assesseurs* – ***Assessors***) of the Competition College (*Mededingingscollege / Collège de la concurrence*). The Competition College is the decision-making body of the Belgian Competition Authority (*Belgische Mededingingsautoriteit / Autorité belge de la Concurrence* - ***BCA***). For each case submitted to the Competition College, a new College is formed by the President of the BCA and two members, who are appointed in alphabetical order within their language group.

All members will be given a mandate of six years. While some of the members are new, others were already part of the outgoing Competition College. The members designated as part of the Dutch language group are Jan Blockx, Isabelle Buelens, Kris Dekeyser, Gerben Pauwels, Pieter Van Cleynenbreugel, Carmen Verdonck, Chris Verleye, and Frank Wijckmans. The members designated as part of the French language group are Laurent De Muyter, Alexandre de Streel, Martin Favart, Christian Huveneers, Norman Neyrinck, Grégoire Ryelandt, Elisabeth van Hecke – de Ghellinck, and Alexis Walckiers.

Although it is public knowledge that a replacement is sought for the current President of the BCA (*See*, this Newsletter, Volume 2021, No. 7), no decision has yet been adopted in this respect. This means that Jacques Steenbergen will continue in his current role of President until further notice.

© 2022 Van Bael & Bellis

DATA PROTECTION

Belgian Data Protection Authority Reprimands Employment Agency for Late Deletion of Job Seeker Data

In a decision of 3 January 2022, the Litigation Chamber (*Geschillenkamer / Chambre Contentieuse* – the ***Litigation Chamber***) of the Belgian Data Protection Authority (*Gegevensbeschermingsautoriteit / Autorité de protection des données* – the ***DPA***) examined two complaints lodged against a private employment agency (the ***defendant***) by one of its former job seekers (the ***complainant***). The complainant had requested that his personal data be deleted from the defendant's database, after not having been recruited.

Background

The complainant was interviewed by the defendant in the fall of 2019 as a candidate for a temporary worker position but was in the end not recruited. The complainant subsequently asked for his personal data to be deleted. On 2 March 2020, the complainant received an e-mail from the defendant, informing him that a personal account on the defendant's online portal had been created. The complainant reacted the same day, stating that he did not need such an account and requested again that all his personal data be deleted from the defendant's databases.

On 3 March 2020, the defendant expressly confirmed that all personal data had been deleted. However, later that day, the complainant received an e-mail from a local office of the defendant regarding a new job vacancy. On 15 April 2020, the complainant received yet another job offer via e-mail. The complainant then decided to file a complaint with the DPA.

DPA's decision

First, the DPA found that the complainant's subscription to the agency's mailing list for job vacancies falls within the tasks of a private employment agency and is therefore based on the performance of a contract with the data subject. According to the DPA, this processing does not infringe Article 6 of General Data Protection Regulation 679/2016 (the ***GDPR***).

However, the way in which the defendant processed the complainant's request for erasure is not compatible with the duty of the controller to facilitate the exercise of the rights of data subjects in accordance with Article 12 (2) of the GDPR and its responsibility to take appropriate organisational and technical measures in this regard.

The DPA noted that the defendant's employee who had received the complainant's erasure request had not transferred the request to the department in charge of handling these requests. As a consequence, the complainant's erasure request had not been registered or processed (contrary to what an employee of the defendant wrote in an e-mail to the complainant), which is why his job-seeker profile remained in the central database. The defendant stated that it wanted to limit the manual processing of these requests for erasure and that it was aiming to process such requests automatically in the future. However, according to the DPA, this "aiming" at automated processing of erasure requests was not compatible with Article 12 (2) of the GDPR. The defendant had to take appropriate technical and organisational measures to ensure and demonstrate that the processing of such requests is carried out in accordance with the GDPR.

Moreover, because the complainant received other e-mails regarding job vacancies after exercising his right of erasure, the DPA found that the defendant breached Articles 12 (2) and 17 of the GDPR. The DPA also held that the defendant did not respect its duty of accountability in breach of Article 5 (2) of the GDPR.

Based on the foregoing, the DPA reprimanded the defendant for failing to comply with the complainant's erasure request. The Belgian DPA considered some mitigating factors, such as the fact that the defendant (i) apologised to the complainant and emphasised that his personal data had been deleted from its database and (ii) promptly granted the complainant's request following the DPA's intervention. The DPA also noted that there was no evidence showing that this had been a deliberate violation,

© 2022 Van Bael & Bellis

and that the incident seemed to be an isolated case. Moreover, the defendant implemented the necessary measures to prevent similar events from happening in the future.

This decision sheds light on the decision-making practice of the Belgian DPA and illustrates the mitigating factors which the DPA may consider when assessing whether or not to impose a fine. The decision can be consulted in Dutch and in French.

European Data Protection Supervisor Indicts European Parliament for Cookie Violations and Illegal Transfers of Personal Data

On 5 January 2022, the European Data Protection Supervisor (***EDPS***) issued a decision reprimanding the European Parliament (the ***EP***) for infringing several provisions of Regulation (EU) 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (***Regulation 2018/1725***). The decision follows several complaints submitted to the EDPS between October 2020 and April 2021 by Members of the EP (***MEPs***) and the non-governmental organisation "None of Your Business" – European Center for Digital Rights (***NOYB***) (together, the ***Complainants***).

Background

The Complainants alleged that the EP's use of cookies on the website https://europarl.ecocare.center (the *Website*), which coordinates COVID-19 PCR testing within the EP premises, violated European rules on data protection. The Website was set up by a third-party provider. The EDPS raised some issues relating to the privacy notices published on the Website and inquired, in particular, about the purpose of a unique identifier stored on the website together with a cookie.

The Complainants made four specific allegations. First, they claimed that the Website incorporated third-party cookies, including several trackers, of companies located in the US (Google and payment provider Stripe). This raised issues regarding the transfer of MEPs' personal data to the US. Second, the Complainants alleged that the Website presented two different data protection notices that were in violation of the transparency and information requirements set out in Regulation 2018/1725. Third, the Website used a different cookie banner depending on the language setting and these cookie banners prompted them to click on the button "accept all cookies". Fourth, the Complainants alleged that their right of access to their personal data had not been satisfied.

The EDPS followed the majority of the complaints. In particular, it held that essential information was missing on the data protection notice, such as the data retention period.

The EDPS decision also contains an interesting assessment of the international transfers in the context of the use of tracking cookies. In particular, it considered that the tracking cookies used, such as Stripe and Google analytics cookies, involve the processing of personal data. Moreover, personal data processed through these cookies were transferred to the US, where the cookie provider was located and hosted all relevant data. While the transfer of personal data relied on Standard Contractual Clauses (***SCCs***), the EDPS stressed that SCCs do "*not substitute the individual case-by-case assessment*" which must be carried out by the data controller, "*in accordance with the Schrems II judgment, to determine whether (...), the third country of destination affords the transferred data an essentially equivalent level of protection to that in the EU.*" If such a level of protection is not guaranteed, the data controller must implement appropriate safeguards in the transfer tool. The EDPS concluded that the EP had failed to demonstrate that the appropriate measures had been adopted to ensure an equivalent protection for the personal data transferred to the US.

The EDPS concluded that the cookie banners in all three languages were not in line with the definition of consent laid down in Regulation 2018/1725. According to Article 5(3) of Directive 2002/58/EC (the ***ePrivacy Directive***), tracking cookies from social plug-ins, third party advertising and analytics clearly requires the data subject's consent. These types of cookies are not strictly necessary to provide a functionality explicitly requested by the user. Furthermore, the cookie banners failed to provide transparent information on the processing of personal data (*i.e.,* the cookie banner did not list all cookies that were used).

© 2022 Van Bael & Bellis

Based on this assessment, the EDPS issued a reprimand to the EP and ordered it to update its data protection notices within one month. The decision of the EDPS is available here.

European Data Protection Board Publishes Guidelines on Right of Access

On 28 January 2022, the European Data Protection Board (***EDPB***) adopted draft guidelines 01/2022 on the data subjects' right of access (the ***Guidelines***). The right of access of data subjects is enshrined in Article 8 of the European Union Charter of Fundamental Rights (the ***Charter***) and has been refined and strengthened in Article 15 of General Data Protection Regulation (EU) 2016/679 (the ***GDPR***).

The Guidelines provide clarifications on the scope of the right of access, what to include in a response to the data subject, the format of the access request, the main methods for providing access, and the notion of manifestly unfounded or excessive requests.

Right of access in general

The GDPR distinguishes three different components of the right of access: (i) confirmation as to whether data about the person is processed or not; (ii) access to this personal data (if any); and (iii) access to information about the processing, such as purpose, categories of data and recipients, (envisaged) duration of the processing, data subjects' rights, and appropriate safeguards in case of third country transfers.

In view of this, the overall aim of the right of access is to provide individuals with sufficient, transparent and easily accessible information about the processing of their personal data, regardless of the technologies used. By exercising this right, data subjects can be aware of and verify the lawfulness of the processing and the accuracy of the processed data. The right of access is thus closely linked with other provisions of the GDPR, in particular with data protection principles including the fairness and lawfulness of processing, the controller's transparency obligation and other data subject rights provided for in Chapter III of the GDPR. After having received access to his/her data, a data subject can more easily exercise other rights such as the right to erasure or rectification (*i.e.*, without it being a prerequisite to exercise the right of access first).

A data subject is not required to explain the reasons for exercising the right of access. It is thus not up to the controller to analyse whether the request will actually help the data subject to verify the lawfulness of the relevant processing or to exercise other rights.

Assessment of access requests

The controller must assess each request individually and must evaluate (i) whether the request concerns personal data linked to the requesting person (*i.e.*, anonymous data does not concern personal data); (ii) whether the request falls within the scope of Article 15 GDPR; and (iii) whether other, more specific, provisions that regulate access in a certain sector apply (for example, a request for access to a banking account history falls under the Payment Services Directive 2015/2366). Also, an assessment must be made of whether the data subject wishes access to all or only parts of the information processed about him/her. Data controllers are encouraged to implement internal procedures for handling access requests.

Regarding the form of the access request, the GDPR does not impose any requirements on data subjects. However, the EDPB encourages data controllers to provide the most appropriate and user-friendly communication channels that facilitate an effective request but are not mandatory.

In order to ensure the security of processing and minimise the risk of unauthorised disclosure of personal data, the controller should identify the data subject and the link between the data subject and the categories of data to which access is requested. In case a controller is unable to identify the data subject, the data subject should be given the opportunity to provide additional information to demonstrate his or her identity. But any request to provide additional information must be proportionate, meaning that such additional information should not be more than what is necessary to verify the data subject's identity. The EDPB emphasises that the use of a copy of an identity document as part of the authentication process creates a security risk for personal data. Also, a copy of an identity card should generally not be considered an appropriate way of authentication. Alternatively, the controller may implement a quick and effective security measure to identify a data subject who has been previously authenticated by the controller (*e.g.,* via e-mail or text message containing confirmation links, security questions or confirmation codes).

© 2022 Van Bael & Bellis

Requests of access can be made via third parties or proxies. For instance, this will be the case if parents/guardians exercise this right on behalf of children. The best interests of the child should be the leading consideration in all decisions taken with respect to access questions involving children.

Scope of right of access

The definition of "personal data" in Article 4(1) GDPR determines the scope of the right of access. This definition was discussed in several Article 29 Working Party documents and has been interpreted by the Court of Justice of the European Union (***CJEU***) on several occasions. For instance, in *Peter Nowak v. Data Protection Commissioner* (Case C-434/16), the CJEU found that written answers submitted by a candidate at a professional examination and any comments of an examiner with respect to those answers constitute personal data concerning the exam candidate (*See*, this Newsletter, Volume 2018, No. 1). The EDPB adds that access must be granted to the actual personal data. A general description of the data will not be sufficient.

In addition to providing access to the personal data themselves, the controller must also offer information on the processing and on data subject rights according to Article 15(1)(a) to (h) and Article 15(2) GDPR. This means referring to information about the processing purpose, categories of data and recipients, (envisaged) duration of the processing, data subjects' rights, and appropriate safeguards in case of third country transfers. Most, if not all, of this information is normally contained in the controller's privacy notice drafted in accordance with Articles 12 to 14 GDPR.

How to provide access?

The appropriate way to provide access may vary depending on the amount of data and the complexity of the processing. Still, the controller must always search for (all) personal data about the data subject throughout its IT systems and non-IT filing systems. In line with Article 25 GDPR on data protection by design and by default, the controller should already have implemented functions enabling the compliance with data subject rights. This implies that there should be appropriate ways to find and retrieve information regarding a data subject when handling a request.

The main way of providing access is giving the data subject a copy of its personal data. However, other methods, such as oral information, inspection of files, onsite or remote access to the data, can under certain circumstances be more appropriate. Also, the controller may choose, depending on the situation at hand, to provide the copy of the data undergoing processing, together with the supplementary information, in different ways (*e.g.,* by e-mail, physical mail, or by the use of a self-service tool). A "layered approach" for providing access may be useful when the amount of the data is significant, which also may facilitate the data subject's understanding of the data. In this case, the first layer should include information about the processing and data subject's rights according to Article 15(1)(a) to (h) GDPR and Article 15(2) GDPR as well as a first part of the processed personal data. In a second layer, more personal data should be provided.

According to Article 12(1) GDPR, information under Article 15 GDPR should be provided in writing, or by other means, including, where appropriate, by electronic means. What could be considered as a commonly used electronic form should be based upon the reasonable expectations of the data subjects and not upon what format the controller uses in its daily operations. This means that the data subject should not be obliged to buy specific software in order to obtain access to the information.

Importantly, an access request should be honoured as soon as possible and in any event within one month of receipt of the request. Certain circumstances may justify an extension of two further months, provided the data subject has been informed about the reasons for such delay within one month following receipt of the request by the controller.

Limits to and restrictions of right of access

In some cases, the right of access can be restricted. In this regard, the following provisions are relevant:

1. Article 15(4) GDPR. According to this provision, the right to obtain a copy should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and, in particular, the copyright protecting the software. However, these consid-

© 2022 Van Bael & Bellis

erations should not give rise to a refusal to provide all information to the data subject. For example, information concerning others can be made illegible.

2. Article 12(5) GDPR. This provision enables controllers to override access requests that are manifestly unfounded or excessive. However, these concepts must be interpreted narrowly, as the principles of transparency and cost-free data subject rights must not be undermined.

3. Article 23 GDPR. The scope of the obligations and rights provided for in Article 15 GDPR may be restricted by way of legislative measures in Union or Member State law. Several Member States, including Germany and Poland, have made use of this option.

The Guidelines are open for public consultation until 11 March 2022 and can be found here.

Re-use of Twitter Data: Belgian Data Protection Authority Fines Non-governmental Organisation for "Fake News" Study

On 27 January 2022, the Belgian Data Protection Authority (the ***DPA***) imposed a fine on the Non-governmental Organisation (***NGO***) EU DesinfoLab (***EU DesinfoLab***) and one of its volunteer researchers (together the ***defendants***), for infringing General Data Protection Regulation (EU) 2016/679 (the ***GDPR***) while studying tweets posted on Twitter concerning the "*Benalla affair*", an incident which caused a big stir in media attention in France and internationally.

The Benalla Affair and Research into Fake News

EU DesinfoLab is a Belgian NGO which tackles disinformation campaigns and "fake news". In 2018, French media revealed a series of incidents relating to Alexandre Benalla, a security officer to French president Emmanuel Macron. Noticing an unusually large social media activity following the Benalla affair, it analysed Twitter messages on the topic in a study called "*Affaire Benalla. Les resorts d'un hyperactivisme sur Twitter*" (free translation: "*Benalla Affair. The means of Twitter hyperactivism*"). The study investigated how and why the affair was such a big topic on Twitter and whether disinformation played an important role in it. As part of their research, the defendants analysed the political profile of the authors of tweets relating to the affair and established that some could be linked to Russian media such as "Russia Today" and "Sputnik". Faced with criticism after publication of the study, the defendants published raw data, including the Twitter profiles of a large number of people.

Following this, a number of data subjects filed complaints with the DPA and its French counterpart, the Commission Nationale d'Information et Libertés (***CNIL***) in relation to: (i) the re-use of personal data from 55,000 Twitter accounts to carry out the study (in which more than 3,300 accounts were politically classified); and (ii) the online publication of files containing the raw data of the study.

Since EU DesinfoLab has its seat in Belgium, the DPA acted as lead supervisory authority.

Exemptions for Journalism and Scientific Research?

In its assessment of the case, the DPA distinguished between two processing activities: (i) the study by EU DesinfoLab which is based on personal data made public on Twitter; and (ii) the online publication of Excel files with raw data on which the study was based, containing large amounts of personal data.

In response to complaints that the processing was not transparent and data subjects did not receive clear information regarding the processing activities, the defendants referred to the exemptions governing the processing for journalistic and/or scientific purposes.

The DPA assessed these exemptions and held that the defendants could not rely on that for scientific research because this requires additional safeguards pursuant to Article 89 of the GDPR, such as pseudonymisation. Such safeguards, and indeed any significant form of internal or external documentation of data protection compliance, was missing. In the absence of appropriate documentation, the DPA held that the defendants could not rely on the exemption for scientific research.

Regarding the exemption for journalistic purposes, the DPA noted that this exemption had not been implemented in Belgian law at the time of the events. While a later Belgian rule limits this exemption to data controllers that are subject to a journalistic ethics code, this was not the case

© 2022 Van Bael & Bellis

at the time when the facts took place. As a result, the DPA held that the defendants could rely on this exemption and therefore did not have to inform data subjects, provided the additional criteria were met. The DPA went on to state that EU DesinfoLab was exempted from this obligation as this could have jeopardised the study and its subsequent publication.

What with the data made publicly available on Twitter?

Regarding the legal basis for the processing, the defendants asserted that the research relies on data that is available for everyone on Twitter and had been posted there by the data subjects themselves. Conscious of the fact that publication is often considered to amount to consent for further use, the DPA took the opportunity to clarify that personal data published on social media is still protected under the GDPR. This means that public data must still comply with the purpose limitation principle unless an exemption applies.

The exemptions to the purpose limitation principle apply if the new purpose is compatible with the original purpose. If this is not the case, the processing must be justified by the data subject's consent or another legal basis, including the controller's legitimate interests.

The DPA recognised that the study pursued a legitimate interest of the defendants. However, to rely on Article 6.1.f of the GDPR (*i.e.*, the legal basis of "legitimate interests"), the processing must (i) be limited to what is strictly necessary for this purpose; and (ii) the legitimate interests should be balanced against the rights and freedoms of the data subjects. The DPA held that this necessity criterion was not met when the defendants published the raw data. However, considering the absence of pseudonymisation and the potential significant impact of this publication on the data subjects (the DPA mentions risks of discrimination and reputational harm), the DPA concluded that the defendants could not rely on Article 6.1.f of the GDPR as a legal basis permitting the publication of raw data supporting their study. Indeed, it held that the risk for the data subjects outweighed the controllers' legitimate interests and the controllers had implemented insufficient safeguards (such as pseudonymisation) to counteract the risks for the data subjects.

Moreover, in order to rely on the "journalism exception", the data controller must conduct a case-by-case assessment of the balance between the right to journalistic freedom of expression (contribution to a debate of general interest) and the right to data protection (impact of the publication). The DPA found that such a case-by-case balancing had not been possible from the outset in view of the large amount of Twitter accounts involved (55,000).

Importance of GDPR documentation

As mentioned above, the DPA considered that the defendants did not have adequate documentation of their data protection compliance. For instance, the parties did not have a clear data protection notice, they had no record of processing activities, and the contracts with the data processors were missing.

Moreover, the DPA considered that the defendants should have carried out a data protection impact assessment as the research at hand clearly involved the "high risk" criteria under Article 35 of the GDPR. Indeed, the research covered a large number of data subjects and included sensitive categories of data, such as political affiliation. The DPA specified that the obligation to conduct a data protection impact assessment applies even if personal data were processed for journalistic purposes.

Sanction

Interestingly, the DPA was initially of the opinion that a warning would suffice, while the CNIL insisted that a fine should be meted out. In its determination, the DPA considered attenuating factors, such as the fact that the defendants had improved their GDPR compliance in response to the inquiry, their public apology, and the fact that the exemptions for journalistic and scientific purposes had not been implemented under Belgian law. But the DPA also took into account aggravating factors, including the seriousness of the infringement (considering that it relates to basic principles of the GDPR), the large number of data subjects, and the sensitive nature of the data (including political affiliation or opinion). On this basis, the DPA imposed a fine of EUR 2,700 on DesinfoLab and of 1,200 EUR on its collaborator.

© 2022 Van Bael & Bellis

This decision serves as a reminder that public information does not fall outside the scope of the GDPR, even if the data are used with the best intentions and for journalistic or scientific purposes.

Belgian Data Protection Authority Finalises Recommendation on Biometric Data Processing

On 6 December 2021, the Belgian Data Protection Authority (***DPA***) published the final version of its recommendation on the processing of biometric data (the ***Recommendation***). The Recommendation follows the DPA's earlier draft rec-ommendation of 15 July 2021 (*See*, this Newsletter, Volume 2021, No. 7). The Recommendation took into account the comments submitted by stakeholders during the public consultation.

The Recommendation provides guidance to data controllers and processors as to the correct application of the rules of General Data Protection Regulation 2016/679 (the ***GDPR***) to the processing of biometric data. Furthermore, the Recommendation invites the federal Parliament to provide for a statutory basis for the processing of biometric data, which, according to the DPA, is currently still lacking, even though this lacuna had already been highlighted by the DPA in its draft recommendation.

Background

The GDPR defines biometric data as personal data that are derived from physical, physiological, or behavioural characteristics of a natural person. This includes data such as digital fingerprints or iris scans. Biometric data are increasingly being used by governments, but also private companies, to identify or authenticate data subjects.

By their very nature, these data are particularly sensitive. Therefore, as a rule, their processing is prohibited under the GDPR, unless the processing can be justified based on one of the exceptions contained in Article 9(2) GDPR.

Lack of statutory basis for processing of biometric data

The Recommendation explores two possible statutory bases that would allow for the processing of biometric data: (i) the data subject's explicit and freely given consent; or (ii) a reason of overriding public interest. This prompted the DPA to conclude that there is currently no legal basis under Belgian law for the processing of biometric data for the authentication of individuals.

First, the statutory basis associated with a "reason of overriding public interest" can only be relied on in relation to the Belgian electronic passport (eID) and European passports. No other laws exist that allow to rely on a reason of overriding public interest.

Second, the DPA highlighted the term "consent" under the GDPR. Consent must be freely given, specific, and informed. It must be unambiguous that the data subject agrees to the processing of his/her personal data. For biometric data, the consent must be explicit. Concerning the requirement that consent must be "freely given", the DPA indicated that this implies a "real choice" for the data subject. This could be problematic in the context of employer-employee relationships since employees may feel pressured to give their consent. The processor of biometric data will then also have to evaluate the balance of power between him and the data subject. If an imbalance exists, the processing will not have a statutory basis.

Other important points

1. The Recommendation, unlike the draft recommendation of July 2021, does not mention a transitional "grace period" during which the DPA would not act against the processing of biometric data without a statutory basis. This grace period was intended to allow the federal Parliament to fill the legislative gap. Consequently, processing biometric data without statutory basis can give rise to sanctions by the DPA.

2. Behavioural characteristics, such as gait pattern or keyboard, touch screen or mousepad use patterns, can constitute biometric data if they allow for the identification of the individual concerned. This must be assessed on a case-by-case basis.

3. The "household exception" of the GDPR, which allows for the processing of personal data by a natural person in the context of a purely personal or household activity, only applies to limited scenarios (*e.g.*, if biometric authentication (*e.g.*, face ID) is used on smartphones or other devices as an alternative for a pin code authenti-

© 2022 Van Bael & Bellis

cation when all conditions are fulfilled). In the context of an employer-employee relationship, the household exception cannot apply.

4. A data protection impact assessment (***DPIA***) will be required for the processing of personal data for the unique identification of data subjects located in public spaces or in private spaces that are publicly accessible. In addition, a DPIA will also be necessary if biometric data are used with "new technologies" prone to creating a high risk to the rights and freedoms of natural persons (Article 35 of the GDPR).

The Recommendation is available in Dutch and French.

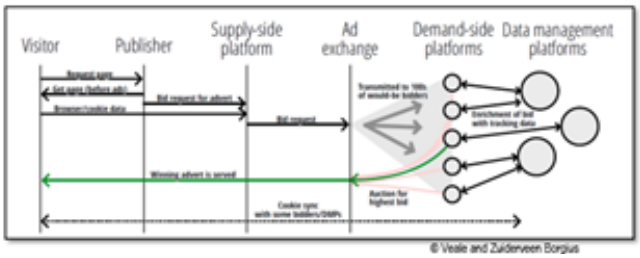
IAB Europe's Transparency and Consent Framework Infringes General Data Protection Regulation and Prompts Belgian Data Protection Authority to Impose Fine of EUR 250,000

The Transparency and Consent Framework (***TCF***), developed by Interactive Advertising Bureau Europe (***IAB Europe***), is a widespread mechanism facilitating the management of users' preferences for online personalised advertising. On 2 February 2022, the Litigation Chamber (*Geschillenkamer / Chambre Contentieuse* – the ***Litigation Chamber***) of the Belgian Data Protection Authority (*Gegevensbeschermingsautoriteit / Autorité de protection des données* – the ***DPA***) imposed a fine of 250,000 EUR on IAB Europe for the TCF's breach of the General Data Protection Regulation 679/2016 (the ***GDPR***). The DPA's decision may have an important impact on the digital advertising industry which relies on the TCF mechanism when deploying the real time bidding process (***RTB***) for online advertisements.

Background and Functioning of the TCF Mechanism and RTB

IAB Europe is a digital marketing trade association – representing corporate members as well as national associations - which indirectly represents 5,000 companies. IAB Europe developed the TCF as a consent solution for digital advertisers to comply with Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the ***e-Privacy Directive***). The TCF also aims to ensure compliance with the GDPR for organisations relying on the OpenRTB protocol. That protocol was developed by IAB Tech Lab which is based in New York. The TCF mechanism and the OpenRTB protocol are connected and, together with Google's AdBuyers protocol, the OpenRTB protocol is the most widely used RTB protocol worldwide.

The OpenRTB protocol is a standard protocol that aims to simplify the interconnection between advertising space providers, publishers, and competing buyers of advertising space. The overall aim is to establish a common language for communication between buyers and vendors of advertising space. RTB refers to the use of an instantaneous automated online auction for the sale and purchase of online advertising space. Practically, when users access a website or application that contains an advertising space, technology companies representing thousands of advertisers can instantly (*i.e.*, 'in real time') bid behind the scenes for that advertising space through an automated auction system using algorithms, in order to display targeted advertising specifically tailored to that individual's profile. Through RTB, billons of advertisement spaces are auctioned every day. The DPA refers to a schematic representation of the RTB process:



When users visit a website or application for the first time, an interface (*i.e.*, a Consent Management Platform or ***CMP***) will pop up where they may consent to the collection and sharing of their personal data, or object to various types of processing based on the legitimate interests of advertising tech vendors. This is where the TCF plays a role: it facilitates the capture and storage of the users' preferences through the CMP. These preferences are then coded and stored in a unique Transparency and Consent string (***TC string***), which will be shared with the organisations participating in the OpenRTB mechanism in order for them to know what the user has consented or objected to. The author of the preferences is identifiable due to the CMP placing a cookie on the user's device. This means that the IP address of the user is identifiable after the TC string and that cookie have been combined.

© 2022 Van Bael & Bellis

The DPA investigated the TCF following a series of complaints filed against IAB Europe in 2019. The complaints mainly claimed that users were insufficiently aware that their profiles are sold a number of times a day to a large number of potential advertisers in order to offer them personal advertising.

DPA Decision

In its decision, the DPA found that IAB Europe acts as a (joint) controller for the TCF system and therefore could be held responsible for the system's infringement of the GDPR.

DPA Decision - IAB Europe is Responsible as Controller of the TCF

First, the DPA held that IAB Europe acts as controller with respect to the registration of individual users' consent signals, objections and users' preferences by means of a TC string. The DPA considered that the TC string is linked to an identifiable user and IAB Europe is the entity that determines the purposes and means of the processing of that personal data (*i.e.*, it determines the means of generating, storing and sharing the TC string).

In its defence, IAB Europe argued that identification codes assigned to users cannot be considered personal data. IAB Europe also raised the point that, since it did not process, own or make decisions on the data, it should not be considered to be a controller.

The DPA disagreed. First, it explained that information should be considered personal data as soon as that information, due to its content, purpose or effect, can be linked to an identified or identifiable data subject by such means that can reasonably be used, regardless of whether the information from which the data subject can be identified is held entirely by the same controller. Second, since publishers and advertising tech vendors would not be able to achieve the goals set by IAB Europe without the TCF, IAB Europe has responsibility as the controller over the users' personal data. It considered that IAB Europe acts as the "managing organisation" for the TCF by determining the policies and technical specifications of the TCF.

IAB Europe's framework thus plays a decisive role in determining the means and purposes of processing users' preferences, consents and objections, regardless of whether IAB Europe handles the personal data itself. The DPA referred to the broad scope of the concept of a "controller" as set out in the case law of the Court of Justice of the European Union (***CJEU***), including *Wirtschaftsakademie* (Case C-210/16; *See* our Newsletter, VBB on Belgian Business Law, Volume 2018, No. 6).

In addition, the DPA referred to the CJEU's judgment and the Advocate General's opinion in the Fashion ID case (Case C-40/17; *See* our Newsletter VBB on Belgian Business Law, Volume 2019, No. 8). The CJEU held that if two parties take converging decisions relating to a processing operation, both can be regarded as controllers. On this basis, the DPA considered that IAB Europe provides an ecosystem within which the consent, objections, and preferences of users are collected and exchanged not for its own purposes or self-preservation. IAB Europe collects and exchanges these in order to facilitate further processing by third parties (*i.e.,* publishers and advertising tech vendors). Therefore, the DPA held that IAB Europe acts as a joint controller together with online advertising firms when the personal data are used in the advertising system in the context of the CMP.

DPA Decision - IAB Europe's TCF Infringes Several Provisions of the GDPR

According to the DPA, as a data controller, IAB Europe must abide by the GDPR which had clearly not been complied with in the case at issue. The DPA found that IAB Europe had breached several provisions of the GDPR as follows:

- Lawfulness. The DPA found that IAB Europe had failed to establish a legal basis for the processing of user personal data through the TCF and RTB platform. Furthermore, no adequate legal grounds were offered by the TCF for the subsequent processing by advertising tech vendors. Users were unable to properly consent to the processing of their personal data due to the lack of information (see *infra*). Furthermore, the legitimate interest of online advertising firms cannot

© 2022 Van Bael & Bellis

constitute a legal basis for processing in the context of direct marketing and behavioural advertising. The DPA found that the legitimate interest of the organisations participating both in the TCF and the OpenRTB protocol did not outweigh the protection of the fundamental rights and freedoms of the data subjects.

- Transparency and information of the users. The information provided through IAB Europe's TCF system did not comply with the GDPR. In this regard, the DPA reasoned that it is difficult for users to maintain control over their personal data under the mechanism, as the information provided through the CMP interface was "*too generic and vague to allow users to understand the nature and scope of the processing, especially given the complexity of the TCF*". Also, users were not informed about the specific purposes for which advertising tech vendors would process their data.

- Accountability, security and data protection by design and by default. The DPA furthermore found that IAB Europe had failed to guarantee the integrity of processing users' preferences, consents and objections and failed to monitor vendors for compliance with their TCF rules. Advertising tech vendors would receive a consent signal without any technical or organisational measure to ensure that this consent signal was valid or that a vendor had actually received it (rather than generated it). The DPA held that in the absence of organisational and technical measures in accordance with the principle of data protection by design and by default, the conformity of the TCF with the GDPR had not been adequately warranted or demonstrated.

- Other obligations pertaining to a controller processing personal data on a large scale. The DPA also found that IAB Europe had failed to keep a register of processing activities, to appoint a DPO and to conduct a data protection impact assessment (***DPIA***). The DPA considered that a DPIA should have been conducted given the large number of data subjects that come into contact with websites that implement the TCF and given the impact of the TCF on the large-scale processing of personal data in the context of the RTB platform.

DPA Decision - Sanctions

In addition to a fine of 250,000 EUR, the DPA imposed an order on IAB Europe to submit a plan for corrective measures within two months after the date of the decision and issued a daily penalty of 5,000 EUR for any failure by IAB Europe to execute the plan within six months after its approval. Additionally, IAB Europe was ordered to permanently delete all TC strings and other personal data already processed in the TCF "*from all its IT systems, files and data carriers, and from the IT systems, files and data carriers of processors contracted by IAB Europe*".

IAB Europe can appeal the DPA's decision to the Markets Court (*Marktenhof / Cour des Marchés*).

The DPA's decision is available in Dutch, French and English.

© 2022 Van Bael & Bellis

INSOLVENCY

Book XX of Code of Economic Law Is Amended to Enhance Transparency Regarding Position of Filing for Bankruptcy

On 28 November 2021, a law "to make justice more human, faster and stricter" was adopted (*Wet om justitie menselijker, sneller en straffer te maken / Loi visant à rendre la justice plus humaine, plus rapide et plus ferme* - the ***Law***). The Law modified Book XX of the Code of Economic Law (*Wetboek van Economisch Recht / Code de droit économique* – ***CEL***).

The main amendment of Book XX of the CEL makes it possible for enterprise courts to access the information available in the (new) Central Point of Contact for accounts and financial contracts of the Belgian National Bank (*Centraal aanspreekpunt / point de contact central* – the ***CCP***). The CCP is a register containing the bank account numbers and all types of contracts with financial institutions in Belgium for all legal entities (regardless of whether they have their seat in Belgium).

This should allow the enterprise courts to gather more information on the financial position of the company filing for bankruptcy when having to rule on insolvency procedures. Currently, these courts must rely on the information provided by the company filing for bankruptcy (or the third party suing a company for bankruptcy).

The explanatory memorandum to the Law clarifies that enterprise courts can use this information in insolvency procedures to ensure the protection of all stakeholders against the negative impact of a potential bankruptcy.

The Law can be found here.

© 2022 Van Bael & Bellis

INTELLECTUAL PROPERTY

European Union Intellectual Property Office Board of Appeal Holds that Owner of 3D Trade Mark Can Oppose Registration of Figurative Mark

On 15 December 2021, the Board of Appeal (***BoA***) of the European Intellectual Property Office (***EUIPO***) held that the owner of a 3D trade mark could oppose the registration of a figurative mark if it creates a likelihood of confusion with one of the perspectives of the 3D trade mark.

Facts and Procedural Background

On 27 September 2019, European Flipper / Pinball Factory GmbH (***Pinball***) applied for the registration of the figurative mark for the classes of goods 11 (Camping stoves), 12 (Camping cars), 20 (Furniture for camping), 21 (Camping grills), and 39 (Rental of recreational vehicles).

On 3 January 2020, Volkswagen Aktiengesellschaft (***Volkswagen***) filed an opposition against Pinball's registration in accordance with Article 8(1) of Regulation 2017/1001 on the European Union Trade Mark (***Regulation 2017/2001***). Volkswagen argued that Pinball's registration created a likelihood of confusion with its 3D European trade mark (***EUTM***) registered for goods and services in Classes 12 (Camping cars), 14 (Goods of precious metals), 16 (Advertising material), 35 (Retail and wholesale services of motor vehicles' parts), 37 (Reconstruction, repair, servicing of vehicles and their parts), 39 (Rental of recreational vehicles) and 41 (Sporting and cultural activities),

and its international trade mark registration for goods and services in Classes 12 (Camping cars), 14 (Goods of precious metals), 16 (Advertising material), 18 (Goods made from leather), 20 (Furniture for camping), 21 (Camping grills), 25 (Clothing), 28 (Scale model vehicles), 30 (coffee or tea base), 35 (Retail and wholesale services of motor vehicles' parts), and 37(Reconstruction, repair, servicing of vehicles and their parts):

The EUIPO's Opposition Division held that the signs presented a low degree of visual similarity and that there was consequently no likelihood of confusion. Volkswagen appealed the Opposition's Division decision to the BoA.

© 2022 Van Bael & Bellis

BoA Reasoning

The BoA overturned the Opposition Division's decision and explained that the perspectives of the 3D trade mark should have been assessed collectively as they represent the same object from different angles. The BoA added that for a 3D mark to have a distinctive character, it must significantly depart from the norms and customs of the sector concerned. Volkswagen's sign is distinctive as the front of the van is characterised by a divided windshield and the curved V-shape on the bonnet with circular headlights on each side.

Regarding the contested trade mark application, the BoA considered that the verbal element "CULTCAMPER" and the figurative element on Pinball's sign were visually co-dominant. Pinball's sign was deemed almost identical to Volkswagen's, with the small difference of a hardly noticeable peace symbol. The BoA concluded that there was a likelihood of confusion as the relevant public in the EU would perceive Pinball's sign as another version of Volkswagen's sign and not as a separate sign with a different commercial origin.

© 2022 Van Bael & Bellis

In the centre of Europe with a global reach

VAN BAEL & BELLIS

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