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

Legal 500 2019

December 2020

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

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

COMMERCIAL LAW

Entry into Force of Ban on Unbalanced Contract Terms in B2B Relationships

As previously reported (*See, this Newsletter, Volume 2019, No. 2, pp. 3-4* and *this Newsletter, Volume 2019, No. 5, p. 4*), the Law of 4 April 2019 modifying the Code of Economic Law concerning abuses of economic dependence, abusive clauses and unfair market practices between companies (*Wet van 4 april 2019 houdende wijziging van het Wetboek van Economisch Recht met betrekking tot misbruiken van economische afhankelijkheid, onrechtmatige bedingen en oneerlijke marktpraktijken tussen ondernemingen / Loi du 4 avril 2019 modifiant le Code de droit économique en ce qui concerne les abus de dépendance économique, les clauses abusives et les pratiques du marché déloyales entre entreprises* – the ***B2B Law***) inserted new provisions regarding the abuse of economic dependence, significantly unbalanced contract terms and unfair practices in business to business (***B2B***) relationships into the Code of Economic Law.

As also noted in a previous issue (*See, this Newsletter, Volume 2019, No. 3, p. 3*), the B2B Law entered into force gradually. The provisions of the B2B Law prohibiting unbalanced contract terms were the last to enter into force and started to apply to contracts concluded, renewed, or modified after 1 December 2020.

Court of Justice of European Union Holds that Star Taxi App, unlike Uber, provides Information Society Services

On 3 December 2020, the Court of Justice of the European Union (***CJEU***) held that a service putting taxi passengers directly in touch with taxi drivers by means of an electronic application constitutes an "information society service" within the meaning of Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (the ***E-Commerce Directive***) if it does not form an integral part of an overall service which has the provision of transport as its principal component (CJEU, 3 December 2020, Case C-62/19, Star Taxi App).

The CJEU delivered its judgment in response to a question referred for preliminary ruling by a Bucharest Regional Court in a dispute between Star Taxi App SRL (***Star Taxi App***) and the Bucharest Municipal Council. Star Taxi App operates a smartphone app that connects taxi passengers with taxi drivers. The Bucharest Municipal Council had extended the obligation to obtain a prior authorisation to firms "dispatching" activities to operators of IT applications such as Star Taxi App. As it did not obtain this authorisation, Star Taxi App received a fine of RON 4,500 (approximately EUR 929).

Star Taxi App challenged this fine, as it considered that its activities qualify as information society services and are hence exempt from any prior authorisation or any other requirement having equivalent effect pursuant to Article 4(1) of the E-Commerce Directive. According to this provision "*Member States shall ensure that the taking up and pursuit of the activity of an information society service provider* [is] *not* […] *made subject to prior authorisation or any other requirement having equivalent effect*". However, pursuant to Article 4(2) of the E-Commerce Directive, Article 4(1) is "*without prejudice to authorisation schemes which are not specifically and exclusively targeted at information society services* […]".

In this context, the Bucharest Regional Court sought guidance from the CJEU as to whether:

1. the services provided by Star Taxi App qualify as information society services within the meaning of the E-Commerce Directive; and

2. if Star Taxi App's services are to be regarded as information society services, the obligation to obtain a prior authorisation to undertake "dispatching" activities imposed by the Bucharest Municipal Council complies with EU law.

In its referral decision, the Bucharest Regional Court highlighted the differences between the Star Taxi App and the Uber app, which according to the CJEU does not amount to an information society service, but a transport service. A key consideration in the CJEU's judgment in *Uber* was the fact that the intermediary service provided by Uber formed an integral part of the underlying transport service (*See, this Newsletter, Volume 2017, No. 12, p. 7* and *this Newsletter, Volume 2018, No. 4, p. 8*). In contrast, Star Taxi App does not automatically link a passenger with a taxi. Upon request, the application displays a list of drivers, authorised and licensed to provide taxi services, that are available for a journey. The passenger is then free to choose a driver from that list. Furthermore, Star Taxi App does not determine the fare, which is paid directly to the driver at the end of the journey. Lastly, Star Taxi App does not control the quality of the vehicles and their drivers or the conduct of the drivers.

Given these particularities, the CJEU assessed whether the services provided by Star Taxi App qualify as information society services to which the E-Commerce Directive applies. An information society service is defined as "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*". The CJEU found that, unlike Uber's services, Star Taxi App's services cannot be regarded as "inherently linked" to the underlying transport services. Crucial in that regard was the fact that Star Taxi App does not create a new market for non-professional drivers, but that its platform is limited to licensed taxi drivers who are already active on the market and for whom the use of the application is not a necessity. Additionally, the app does not organise the general functioning of the underlying transport services as it does not select the drivers, set or charge prices or control the vehicles or their drivers. Consequently, the CJEU held that the services provided by Star Taxi App constitute "information society services" as they do not form an integral part of an overall service which has the provision of transport as its principal component.

The CJEU then examined the compatibility with EU law of the prior authorisation requirement to undertake taxi "dispatching" services. In line with Article 4(2) of the E-Commerce Directive, it held that this Directive does not prevent EU Member States from applying a prior authorisation scheme to a provider of an information society service when this scheme does not exclusively and specifically target information society services, but also applies to providers of economically equivalent services. In the case at hand, the Romanian legislation applied to all kinds of "dispatching" services alike, whether provided by telephone or by IT application. Consequently, the ban on prior authorisation laid down in Article 4(1) of the E-Commerce Directive does not apply.

The CJEU also held that Directive 2006/123/EC of 12 December 2006 on services in the internal market (the ***Services Directive***) allows EU Member States to impose prior authorisation as a requirement on providers of services under the same conditions as those applicable to any restriction of a fundamental freedom, *i.e.,* (i) the scheme must not be discriminatory; (ii) it must be justified by an overriding reason relating to the public interest; and (iii) there must not be less restrictive measures capable of achieving the same objective. Accordingly, the CJEU concluded that EU Member States cannot subject the obtainment of a prior authorisation to requirements that are technologically unsuited to the applicant's intended service, which is a matter for the referring court to determine.

Finally, the CJEU held that the prior authorisation requirement does not constitute a technical regulation within the meaning of Article 5 of Directive (EU) 2015/1535 of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services. To qualify as a "technical regulation", the national legislation needs to be "specifically aimed" at information society services. As stated above, the Romanian legislation applied to all kinds of "dispatching" services without distinction. Consequently, Romania was not required to notify the legislation to the European Commission prior to its adoption.

COMPETITION LAW

Bill Bolsters Legal Professional Privilege for Inhouse Counsel

The federal Chamber of Representatives published at the end of December 2020 a private members' bill seeking to amend the Law of 1 March 2000 governing the Belgian Institute of Inhouse Counsel ("*Wetsvoorstel tot wijziging van de Wet van 1 maart 2000 tot oprichting van een Instituut voor Bedrijfsjuristen*"/ "*Proposition de loi modifiant la loi du 1er mars 2000 créant un Institut des juristes d'entreprise*")(the ***Bill***) which can be found here and here.

The Bill proposes new rules governing access to the regulated profession of inhouse counsel and amends the institutional architecture of the Institute of Inhouse Counsel (***IIC***).

Significantly, the Bill also modifies Article 5 of the Law of 1 March 2000 which confers confidentiality on advice given by inhouse counsel ("Legal Professional Privilege" or ***LPP***). The Bill specifies the scope of the confidentiality regime established by Article 5 and adds criminal penalties to parties who fail to observe the confidentiality requirement.

Scope

The more precise definition of the scope of the confidentiality afforded to the advice of inhouse counsel is based on a judgment given by the Brussels Court of Appeal on 5 March 2013 (*See, this Newsletter, Volume 2013, No. 3, p. 2*) and confirmed by the Supreme Court on 22 January 2015 (*See, this Newsletter, Volume 2015, No. 2, p. 2*) in a case regarding a dawn raid carried out by the Belgian competition authorities relating to a competition procedure against Belgacom (now: Proximus). According to a new definition whose language could certainly be improved, the confidentiality of advice will extend to "all information which [inhouse counsel] obtained when giving legal advice as well as to the advice regarding the legal position, the bringing of an action or the averting of such action and the follow-up of a legal procedure". The amended Article 5 adds that the information at issue includes "the advice and all documents and correspondence pertaining to such advice".

Criminal penalties

Pursuant to the amended Article 5, a failure to observe the confidentiality of advice by inhouse counsel may give rise to fines and/or imprisonment. The explanatory note preceding the bill indicates that the criminal penalties may apply to inhouse counsel, but also to "governmental entities and the courts". The question arises whether this provision adds anything to the existing arsenal of criminal provisions governing the duty of secrecy of specific government officials and members of the judiciary. Additionally, if the Bill becomes law, it is likely to exacerbate the tension between EU competition law and Belgian competition law. Under current rules governing LPP, competition advice given by members of the IIC is shielded from inspection by the Belgian Competition Authority, but not from review by the European Commission (the ***Commission***) which relies on EU law to deny LPP to advice given by inhouse counsel. This dichotomy will become more problematic if, at least theoretically, Belgian criminal law may be applied to investigative measures taken by Commission officials that are in breach of Article 5.

CONSUMER LAW

Publication of Collective Redress Directive

As reported in the previous issue of this Newsletter (*See, this Newsletter, Volume 2020, No. 11, p. 7*), on 24 November 2020, the European Parliament adopted a Directive on representative actions for the protection of collective interests of consumers (the "Collective Redress Directive" or ***CRD***).

On 4 December 2020, the CRD was published in the *Official Journal of the European Union*. EU Member States must implement the CRD in their national legal orders by 25 December 2022 and apply the new rules to collective damages claims initiated on or after 25 June 2023.

Winter Sales to Take Place between 4 January 2021 and 31 January 2021

On 10 December 2020, the Federal Government adopted a Royal Decree modifying the sales period within the meaning of Article VI.25, §1, first indent of the Code of Economic Law (*Koninklijk Besluit van 10 december 2020 betreffende de wijziging van de solden periode bedoeld in het artikel VI.25, §1, 1°, van het Wetboek van economisch recht / Arrêté royal du 10 décembre 2020 relatif à la modification de la période des soldes visée à l'article VI.25, §1er, 1°, du Code de droit économique* – the ***Royal Decree***).

Pursuant to Article VI.25 of the Code of Economic Law, companies may sell their products at discounted prices between (i) 3 January (or 2 January when 3 January falls on a Sunday) and 31 January; and (ii) 1 July (or 30 June when 1 July falls on a Sunday) and 31 July.

However, the Royal Decree exceptionally postponed the start of the 2021 winter sales to Monday 4 January 2021, instead of Saturday 2 January 2021, with a view to avoiding large gatherings in commercial premises in order to limit the spread of COVID-19.

CORPORATE LAW

New Rules on Remote Participation and Voting at Shareholders' Meetings

On 20 December 2020, the federal Parliament adopted a law containing various temporary and structural provisions regarding justice in the fight against the spread of Covid-19 (*Wet houdende diverse tijdelijke en structurele bepalingen inzake justitie in het kader van de strijd tegen de verspreiding van het coronavirus Covid-19 / Loi portant des dispositions diverses temporaires et structurelles en matière de justice dans le cadre de la lutte contre la propagation du coronavirus Covid-19* - the ***Law***). The Law introduces a series of measures to facilitate remote participation of and voting by the shareholders or members of limited liability companies (*naamloze vennootschap / société anonyme*), private limited liability companies (*besloten vennootschap / société à responsabilité limitée*), cooperative companies (*coöperatieve vennootschap / société cooperative*) and (international) non-profit associations ((*internationale) vereniging zonder winstoogmerk / association (internationale) sans but lucratif*) in meetings of the shareholders or members.

Currently, the Companies and Associations' Code (*Wetboek van vennootschappen en verenigingen / Code des sociétés et des associations* – the ***BCAC***) provides for the possibility to organise virtual meetings of shareholders and members if these meetings do not fall in the category of meetings that must be held in the presence of a notary public. In addition, the possibility of holding remote meetings should be explicitly provided for in the articles of association. In that case, the terms of participation in such virtual meetings must be clearly spelled out in the articles of association.

The new provisions introduced by the Law amend the BCAC and provide as follows:

- An express authorisation in the articles of association allowing entities to organise virtual meetings is no longer required.

  The decision to organise such virtual meetings now belongs to the management body. For its decision, the management body must take account of the number of shareholders (or members) who would attend such a meeting and the technology which the entity would use.

- Even if a virtual meeting is organised, the entity must still simultaneously hold a physical meeting. Shareholders or members can thus not be forced to attend the meeting virtually.

  This rule is not new and was already provided for in the BCAC. However, it had been lifted between March 2020 and June 2020 during the first Covid-19 lockdown in Belgium. Given the rationale of the Law and the restrictions on public gatherings which will probably continue to apply for at least a few months, it was expected that this rule would be lifted permanently.

- There is no obligation to organise meetings virtually, just a possibility.

- (International) non-profit associations can, in certain circumstances, also adopt written shareholders' resolutions. Furthermore, voting ahead of the meeting is now also allowed.

- Virtual meetings must satisfy four specific conditions: (i) the entity must be able to verify the identity and capacity of the shareholders or members; (ii) the convening notice must contain a clear and precise description of the procedure to attend the meeting; (iii) members of the bureau must attend the physical meeting which is organised simultaneously; and (iv) the means of communication used by the shareholders or members to participate in the meeting must allow them to participate in the discussions directly, simultaneously and without being interrupted. They must also be able to exercise their voting rights and ask questions (this last requirement will only apply from 30 June 2021).

The Law entered into force on 24 December 2020.

DATA PROTECTION

European Data Protection Board Publishes Final Guidelines on Data Protection by Design and Default

On 1 December 2020, the European Data Protection Board (the ***EDPB***) published the finalised version of its guidelines on the principles of Data Protection by Design and Default (*Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*; the ***Guidelines***). The Guidelines were adopted on 20 October 2020 following public consultation of the draft guidelines published on 13 November 2019 (for a discussion of the draft guidelines, *see, this Newsletter, Volume 2019, No. 11, at p. 8*).

The Guidelines explain the obligation of Data Protection by Design and by Default under Article 25 of the General Data Protection Regulation (the ***GDPR***) and provide guidance and examples illustrating these principles. Data Protection by Design and Default is a requirement for all controllers, independent of their size or the complexity of personal data processing. The requirements, therefore, apply to small businesses and multinational organisations alike.

The EDPB indicates that the final version of the Guidelines contains updated wording and further legal reasoning to address comments and feedback received during the public consultation. Here are some of the noteworthy changes in the final version of the Guidelines:

- The Guidelines now clarify that the principles of Data Protection by Design and by Default are "complementary concepts". According to the EDPB, the principles mutually reinforce each other. Data subjects will benefit more from Data Protection by Default if Data Protection by Design is concurrently implemented and *vice versa*.

- The EDPB emphasises that the obligation to maintain, review and update, as necessary, the processing operation also applies to pre-existing systems. This implies that legacy systems designed before the GDPR entered into force are required to undergo reviews and maintenance to ensure the implementation of measures and safeguards that implement the principles and rights of data subjects in an effective manner, as outlined in the Guidelines.

- As regards the examples in the Guidelines and the lists of key elements for each of the principles, the EDPB underlines that these are neither exhaustive nor binding. They are instead meant to be guiding elements for each of the principles. Controllers need to assess how to guarantee compliance with the principles in the context of the concrete processing operation in question. Also, it is the controllers who must implement the basic data protection principles outlined in Article 5 and Recital 39 of the GDPR to achieve Data Protection by Design and Default. These basic data protection principles include transparency, lawfulness, fairness, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability.

- The Guidelines specify how to implement the "state of the art" concept. This concept imposes an obligation on controllers, when determining the appropriate technical and organisational measures, to take account of the progress in technology. Controllers therefore must have knowledge of technological advances and must make sure to stay up to date. Also, controllers need to know how technology can present data protection risks or opportunities to the processing operation, and, how to implement and update the measures and safeguards that secure effective implementation of the principles and rights of data subjects. The "state of the art" criterion also applies to organisational measures. Lack of organisational measures can lower or even undermine the effectiveness of a chosen technology. Examples of organisational measures are the adoption of internal policies, the organising of up-to-date technology training sessions, and maintaining IT security governance and management policies.

The Guidelines include concrete recommendations for data controllers, data processors and producers of products, services, and applications. For instance, controllers should actively involve the Data Protection Officer (***DPO***), if they have one, in the entire planning and processing lifecycle. Also, processors and possibly producers should consider certification of processing operations.

The EDPB recognises the challenges of Data Protection by Design and Default for small and medium enterprises (***SMEs***) and applies a lower threshold to them. SMEs are recommended to (i) conduct early risk assessments; (ii) start with small scale processing and increase scope and sophistication only later; (iii) use partners with a good track record; (iv) talk with Data Protection Authorities (***DPAs***), and be informed about guidance from DPAs and the EDPB; and (v) adhere to applicable codes of conduct.

Finally, the EDPB emphasises the need for a harmonised approach to implementing principles and rights and encourages associations or bodies preparing codes of conduct following Article 40 of the GDPR also to incorporate sector-specific guidance on Data Protection by Design and Default.

A copy of the Guidelines can be consulted here.

European Data Protection Board Publishes Decision to Establish Coordinated Enforcement Framework

On 1 December 2020, the European Data Protection Board (the ***EDPB***) published its decision to create a Coordinated Enforcement Framework (***CEF***) under the General Data Protection Regulation (the ***GDPR***).

National supervisory authorities (***SAs***) play a fundamental role in supervising compliance with the GDPR and have a duty to cooperate. Additionally, coherence in the decisions of SAs will contribute to the free movement of data among the Member States. The EDPB supports a consistent approach through appropriate procedures, regular meetings with SAs and (internal) guidance. In addition, the GDPR established cooperation between SAs and introduced a one-stop-shop mechanism governing cross-border data processing cases. The new CEF supports and builds on mechanisms for cooperation in the GDPR.

The CEF has a broad scope, ranging from joint awareness raising and information gathering to enforcement sweeps and joint investigations. The EDPB consists of the heads of the SAs and the European Data Protection Supervisor (***EDPS***). Each year, the EDPB will decide upon a subject for coordinated action and agree on the methodology for such action. The SAs will determine the scope of national implementation of the annual coordinated action and will carry it out in accordance with the methodology that was agreed upon. The CEF offers a "rulebook" for the coordinated action.

Participation by SAs in the CEF in any given year will not be mandatory. SAs will share progress updates, other relevant information and best practices. The CEF does not alter the other forms of cooperation and consistency mechanisms under the GDPR.

The CEF can be found here.

European Data Protection Board Publishes 2021-2023 Strategy

On 15 December 2020, the European Data Protection Board (the ***EDPB***) adopted its strategy for the period 2021-2023. The EDPB's strategic objectives focus on the following four objectives: (i) enhancing harmonisation and facilitating compliance; (ii) supporting effective enforcement and efficient cooperation between national supervisory authorities; (iii) preserving fundamental rights in the face of new technologies; and (iv) considering the global dimension of data protection.

Enhancing harmonisation and facilitating compliance

The EDPB will continue providing guidance on the key concepts of EU data protection law. To this end, the EDPB will again engage with external stakeholders through stakeholder events and public consultations. The EDPB also encourages the development and implementation of compliance mechanisms for controllers/processors. Codes of conduct and certifications will receive more attention, as well as other awareness raising tools for data subjects (in particular, children) and non-expert professionals, such as SMEs.

Supporting effective enforcement and efficient cooperation between national supervisory authorities

The EDPB intends to support and facilitate the use of the EU General Data Protection Regulation (the ***GDPR***) cooperation and consistency mechanisms. Further, it will promote a common application of critical concepts related to these procedures and work to strengthen the communication between national supervisory authorities (***SAs***) in this setting.

The EDPB plans to implement its Coordinated Enforcement Framework (***CEF***) that was introduced earlier this month, facilitating joint actions in a flexible but coordinated manner using common methodologies (*See, this Newsletter, p. 9*). In addition, the EDPB will establish a Support Pool of Experts to provide specialised support.

Preserving fundamental rights in the face of new technologies

As regards new technologies, the EDPB will establish common positions and guidance in areas such as artificial intelligence, biometrics, profiling, and advertising technology. The EDPB also plans an evaluation of cloud services and blockchain.

The Strategy also announces further guidance on the principle of accountability and on data protection by design and by default. The EDPB will continue cooperating with other regulators, including consumer protection and competition authorities, to ensure that individuals receive optimal protection and to prevent harm.

Considering the global dimension

The EDPB will promote high EU and global standards for international data transfers to third countries in the private and public sectors. To this end, the EDPB will promote the use of transfer tools that ensure an essentially equivalent level of protection for the personal data transferred. Further, the EDPB aims to develop and provide practical guidance regarding these transfer tools. The EDPB will also engage with the international community to promote EU data protection as a global model. Finally, the EDPB will focus on cooperation with supervising authorities from third countries.

The EDPB's 2021-2023 Strategy can be consulted here.

European Data Protection Board Issues First Binding Decision under Article 65 GDPR

On 9 November 2020, the European Data Protection Board (the ***EDPB***) adopted its first binding decision (the ***Decision***) based on Article 65 of the General Data Protection Regulation (the ***GDPR***). The Decision seeks to resolve a dispute that arose following a draft decision issued by the Irish supervisory authority (***SA***) as lead supervisory authority (***LSA***) regarding Twitter International Company and the subsequent relevant and reasoned objections (***RROs***) expressed by several concerned supervisory authorities (***CSAs***).

The Irish SA issued the draft decision following an own-volition inquiry and investigations into Twitter, after the company had notified the Irish SA of a personal data breach on 8 January 2019. The data breach arose from a bug in Twitter's design, due to which, if a user on an Android device changed the email address associated with his or her Twitter account, the protected tweets became unprotected and therefore accessible to a wider public (*i.e.,* not just the user's followers) without the user's knowledge. In May 2020, the Irish SA shared its draft decision with the CSAs in accordance with Article 60(3) of the GDPR. The CSAs then had four weeks to submit their RROs. The CSAs issued RROs on the infringements of the GDPR identified by the LSA, the role of Twitter as the (sole) data controller, and the quantification of the proposed fine.

As the LSA rejected the objections and/or considered they were not "relevant and reasoned", it referred the matter to the EDPB in accordance with Article 60(4) of the GDPR, thereby initiating the dispute resolution procedure (*See, this Newsletter, Volume 2020, No 10, at p. 16* on the EDPB's Guidelines on relevant and reasoned objections under Article 60 of the GDPR).

In its Decision, the EDPB held that, except for objections raised on the insufficiently dissuasive nature of the fine by some CSAs, the Irish SA was not required to amend its draft decision. On the nature of the fine, the EDPB decided that the objections put forward by the CSAs met the requirements of Article 4(24) of the GDPR and that the Irish SA was required to re-assess the elements it relied upon to calculate the amount of the fine to be imposed on Twitter. The Irish SA had to increase the fine to ensure that it satisfied the requirements of effectiveness, dissuasiveness and proportionality established by Article 83(1) of the GDPR and considering the criteria of Article 83(2) of the GDPR. According to these criteria, the SA should consider the nature, gravity and duration of the infringement. In addition, the SA should take account of the actions taken by the controller or processor to mitigate the damage suffered by data subjects and the categories of personal data affected by the infringement.

On 15 December 2020, the Irish SA announced its final decision and found that Twitter infringed Articles 33(1) and 33(5) of the GDPR by failing to notify the breach to the Irish SA within the prescribed timeframe and failing to keep adequate documentation of the data breach. The Irish SA imposed an administrative fine of EUR 450,000 on Twitter as an effective, proportionate, and dissuasive measure.

The EDPB's Decision can be found here.

Belgian Data Protection Authority Publishes Management Plan 2021

On 9 December 2020, the Belgian Data Protection Authority (*Gegevensbeschermingsautoriteit / Autorité de protection des données*; the ***DPA***) released its management plan for 2021 (*Beheersplan / Plan de Gestion*; the ***Management Plan***). The Management Plan translates the strategic and operational objectives contained in the Strategic Plan for 2020-2025 (***Strategic Plan***), which was issued in December 2019 (*See, this Newsletter, Volume 2019, No 12, at p. 7*), and creates concrete objectives for the next year.

By way of introduction, the DPA highlights its accomplishments and challenges of the past year, with a focus on the extensive role played in advising the government and monitoring multiple initiatives in the COVID-19 crisis. This was already highlighted in the DPA's 2019 Annual Report of 30 September 2020 (*See, this Newsletter, Volume 2020, No 10, at p. 15*). Given the increased workload resulting from the entry into force of the General Data Protection Regulation (the ***GDPR***), the DPA asks for a structural increase of its budget.

The Management Plan addresses for each of its five directorates the contribution to the Strategic Plan and their strategic and operational objectives. The five directorates are (i) the General Secretariat (*Algemeen Secretariaat / Secrétariat Général*), (ii) the First-line Service (*Eerstelijnsdienst / Service de Première Ligne*), (iii) the Knowledge Centre (*Kenniscentrum / Centre de Connaissances*), (iv) the Inspectorate (*Inspectiedienst / Service d'Inspection*), and (v) the Dispute Resolution Chamber (*Geschillenkamer / Chambre Contentieuse*).

The Management Plan promises to clarify the role of the Data Protection Officer (***DPO***); develop a toolbox for penalties; and enhance cross-border cooperation with partners both inside and outside the EU.

The Management Plan is available in Dutch and French.

EU-UK Trade and Cooperation Agreement Regulates Data Transfers following Brexit

On 24 December 2020, the EU and the UK reached an agreement in principle on a EU-UK Trade and Cooperation Agreement following Brexit (the ***EU-UK Trade Agreement***).

Regarding data protection, the EU-UK Trade Agreement provides for a further transition period of up to 6 months to enable the European Commission to complete its adequacy assessment of the UK's data protection laws. During this further transition period, personal data can continue to be transferred from the EU to the UK without implementing additional safeguards. As the transition period for the UK's withdrawal from the EU ended on 31 December 2020, this creates the requisite certainty for the immediate future. Since 1 January 2021, the UK has become a third country" for purposes of the General Data Protection Regulation (the ***GDPR***).

Before the EU-UK Trade Agreement was concluded, the European Data Protection Board (the ***EDPB***) had issued a statement on the end of the Brexit transition period in which it describes the main implications of the end of that period for data controllers and processors (the ***Statement,*** which can be found here). Additionally, the EDPB adopted an information note on data transfers under the GDPR after the transition period (the ***Information Note***, which can be found here).

It remains to be seen whether the European Commission will be able to conclude its adequacy review before the end of the 6 months transition period. In the absence of an adequacy decision applicable to the UK by then, all transfers of personal data between parties subject to the GDPR and UK entities will require appropriate safeguards. These include standard data protection clauses, binding corporate rules and codes of conduct. Also, enforceable data subject rights and effective legal remedies for data subjects must be in place. Moreover, controllers and/or processors will have to comply with other obligations under the GDPR. For example, privacy notices will have to mention transfers to the UK.

In our Brexit Q&A, we answer eight frequently asked questions and provide an overview of issues to consider and steps to take in order to be compliant with data protection rules following Brexit in case no adequacy decision is reached.

INSOLVENCY

New Temporary Protection Measures for Enterprises Forced to Close Due to Covid-19 Restrictions

On 20 December 2020, the federal Parliament adopted a law containing various temporary and structural provisions regarding justice in the fight against the spread of Covid-19 (*Wet houdende diverse tijdelijke en structurele bepalingen inzake justitie in het kader van de strijd tegen de verspreiding van het coronavirus Covid-19 / Loi portant des dispositions diverses temporaires et structurelles en matière de justice dans le cadre de la lutte contre la propagation du coronavirus Covid-19* - the ***Law***). The Law includes a statutory moratorium applicable from 24 December 2020 until 31 January 2021 for enterprises that are or were forced to close pursuant to the Ministerial Decree of 1 November 2020 setting out emergency measures to limit the spread of Covid-19 (the ***Moratorium***).

Under the Moratorium enterprises are protected against (i) bankruptcy, judicial dissolution, and transfers under judicial authority; (ii) attachment and enforcement measures; and (iii) the termination of contracts for failure to pay. In addition, payment terms that form part of a homologated judicial reorganisation plan are extended by the term of the Moratorium, which may result in an extension of the general maximum payment term of five years for the implementation of the reorganisation plan.

These protection measures, and their exceptions, are identical to those provided for by the first moratorium which applied between April 2020 and June 2020 following the first lockdown (*See, this Newsletter, Volume 2020, No. 4, p. 16*, and our memorandum of 27 April 2020 which details the temporary protection measures). Unlike this first moratorium, however, the Moratorium only applies to enterprises that are or were forced to close due to the governmental restrictions imposed because of the Covid-19 crisis and whose continuity is threatened by these restrictions.

Unless extended, the Moratorium will end on 31 January 2021.

INTELLECTUAL PROPERTY

According to Court of Justice of European Union Resale of Vehicles and Replacement Parts Constitutes "Genuine Use" of Trade Mark

On 22 October 2020, the Court of Justice of the European Union (***CJEU***) clarified the concept of "genuine use" in response to a referral for a preliminary ruling from a German court in cases C-720/18 and C-721/18 *Ferrari SpA v European Union*. The CJEU answered in the affirmative the question whether the resale of vehicles and replacement parts amounts to a form of "genuine use" of a trade mark pursuant to Article 12(1) of Directive 2008/96/EC (the ***Former Trade Mark Directive***). This provision is now incorporated in Article 19 of Directive 2015/2436.

Factual Background and Procedure

In 1987, Ferrari registered the trade mark "Testarossa" with the World Intellectual Property Organisation as an international trade mark for goods in Class 12 (vehicles; apparatus for locomotion by land, air, or water, in particular motor cars and parts thereof.) The same mark was also registered with the Deutsches Patent -und Markenamt (*German Patent Office and Trade Mark Office*) for goods in Class 12 (land vehicles, aircraft and water vehicles and parts thereof, motors and engines for land vehicles, and car components).

The Regional Court in Düsseldorf ordered the cancellation of both trade marks on the grounds that during a period of five years Ferrari had not made a "genuine use" of the marks in Germany and Switzerland. Ferrari appealed that decision to the Higher Regional Court in Düsseldorf (the ***Referring Court***). According to the Referring Court, Ferrari had used those trade marks to identify replacement parts of luxury sports cars sold under those marks.

CJEU's Answer

The CJUE answered that according to its case-law (C-40/01, *Ansul BV v Ajax randbeveiliging BV*), there can be "genuine use" even if the trade mark is used for goods that had been sold before rather than for newly available ones. This requirement is also fulfilled when the trade mark proprietor makes actual use of the same mark for parts that are integral to the structure of such goods or when goods or services directly connected to the goods previously sold were intended to meet the needs of the costumers. It is thus irrelevant that the registration of the trade mark covers entire goods or replacement parts. There can be a "genuine use" in both cases. The CJEU held that there could be "genuine use" even if the trade mark was only used with luxury sports cars or only with replacement parts of such goods, unless the consumer who wishes to purchase such good would perceive them as a subcategory of goods for which the mark concerned had been registered.

The CJEU further specified that when reselling second-hand goods, the proprietor uses the mark as this guarantees the identity of the origin of the goods and can consequently amount to a "genuine use".

Moreover, the CJEU held that Article 12(1) of the former Trade Mark Directive is to be interpreted in the sense that a trade mark is put to "genuine use" when the proprietor provides specific services connected with the goods previously sold under that mark, on the condition that the services are provided under that same mark.

Lastly, the CJEU held that Article 351 of the Treaty on the Functioning of the European Union (***TFEU***) must be interpreted as allowing a court of a Member State to apply a convention concluded between a Member State and a non-Member State such as the Convention between Switzerland and Germany concerning the Reciprocal Protection of Patents, Designs, and Trade marks (signed in Berlin on 13 April 1982), which provides that a trade mark registered in a Member State that is used in the non-Member state must be taken into consideration to determine whether there is a "genuine use".

The CJEU's judgment can be found here.

Court of Justice of European Union Holds That Emailing Copyright-Protected Content to Court Is No Communication to Public

On 29 October 2020, the Court of Justice of the European Union (***CJEU***) held in case C-637/19, *BY v. CX*, that the transmission to a court of copyright protected works by electronic means (such as emails) does not amount to a "communication to the public" within the meaning of Article 3(1) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (***InfoSoc Directive***.) Moreover, the CJEU affirmed that a balance must be struck between the rights of copyright holders, the protection of the fundamental rights of the users of the works, and the public interest.

Factual Background and Procedure

The request for a preliminary ruling was made by the Svea Court of Appeal (Patents and Market Court of Appeal in Sweden) in a dispute between CX and BY, two natural persons operating a website. In civil proceedings between the parties, CX submitted into evidence a copy of a page of text containing a photograph protected by copyright taken from BY's website. In reaction, BY claimed that this constituted an infringement of copyright and/or related rights.

The Court of First Instance held that the disclosure did not constitute an infringement under Swedish constitutional law on access to documents. BY appealed the decision to the Svea Court of Appeal which in turn asked the CJEU for clarification. It sought to know whether a court could be considered to be a "public" for the purpose of copyright law and whether this concept should be interpreted in the same way in Articles 3 and 4 of the InfoSoc Directive.

CJEU's Reasoning

The CJUE's established case-law concerning Article 3(1) of the InfoSoc Directive is that there are two cumulative criteria to determine "a communication to the public": an act of communication of a work and the communication of that work to the public (case C-117/15 *Reha Training*).

The CJEU held that the first condition is fulfilled when a protected work is transmitted by electronic means to a court as evidence. By contrast, the CJEU maintained that the second condition had not been satisfied. The CJEU followed the Advocate General's opinion that the communication was made to "a clearly defined and closed group of persons holding public service functions within a court". Therefore, no copyright infringement had taken place.

The CJEU added that there must be a fair balance between the interests of holders of copyright, the interests of the users of protected subject matter and the public interest (case C-476/17, *Pelham and Others*). The right to an effective remedy guaranteed by Article 47 of the Charter of Fundamental Rights would be seriously compromised if a copyright holder were able to object to a court disclosure on the sole ground that evidence contains protected subject matter.

The CJEU's judgment can be found here.

LABOUR LAW

Court of Justice of European Union Clarifies Concept of Posted Workers Employed in International Road Transport

On 1 December 2020, the Court of Justice of the European Union (the ***CJEU***) delivered a judgment clarifying the concept of posted workers employed in the international road transport sector in different Member States (case C-815/18, *Federatie Nederlandse Vakbeweging v. Van den Bosch Transporten BV, Van den Bosch Transporte GmbH, and Silo-Tank Kft, see* here).

The case had come before the CJEU following a request for a preliminary ruling from the Supreme Court in the Netherlands ("*Hoge Raad der Nederlanden*") regarding the interpretation of posted workers within the meaning of the Directive 96/71 of the European Parliament and of the Council of 16 December 1996 concerning the posting of workers in the framework of the provision of services (the ***Directive***).

Legal Background

According to Article 3 (1) of the Directive "*Member States shall ensure that, whatever the law applicable to the employment relationship, the undertakings* [which, in the framework of the transnational provision of services, post workers to the territory of a Member State] *guarantee workers posted to their territory* [an essential number of] *terms and conditions of employment* (…) *which, in the Member State where the work is carried out, are laid down by law, regulation or administrative provision and/or by collective agreements or arbitration awards which have been declared universally applicable* (…)". The minimum terms and conditions of employment to be guaranteed to posted workers in the framework of this article concern, for example, the maximum duration of work, the minimum rates of pay (including overtime rates) and the health and safety measures at work.

Factual Background

A transport company located in the Netherlands (Company A) had concluded charter contracts for international road transport operations with a company located in Germany (Company B) and a company located in Hungary (Company C). All companies belonged to the same group of companies.

Company A is a member of the Netherlands Association for Goods Transport and was covered by the collective labour agreement applicable to that sector (the ***CLA***), concluded between that association and the Netherlands Federation of Trade Unions (the ***NFT***). The CLA was not declared universally applicable. A second collective labour agreement, applicable to the professional goods transport by road sector, the provisions of which were essentially identical to those of the CLA, had been declared universally applicable, unlike the CLA. However, under national Dutch law, undertakings covered by the CLA were exempt from the second collective labour agreement only if they complied with the CLA.

German and Hungarian employees who were employed by the companies B and C as drivers were not granted the employment conditions provided for by the CLA, even though they were carrying out transport operations under the charter contracts. As a rule, during the period concerned, the charter operations started in the Netherlands and the journeys ended there, but most of the transport operations carried out under the charter contracts at issue took place outside the territory of the Netherlands.

According to the NFT, when Company A used drivers coming from Germany and Hungary, it had to apply to them the basic conditions of employment under the CLA, in their capacity as posted workers within the meaning of the Directive.

The NFT brought an action against Companies A, B and C before the competent Dutch Court of First Instance requiring those companies to comply with the CLA towards the drivers. In an interim judgment delivered at first instance, it was held that the basic conditions of employment under the CLA should be applied to the drivers coming from Germany and Hungary whose services had been used by Company A.

The Dutch Court of Appeal overruled this judgment, considering that the charter contracts fell outside the scope of the Directive, as the employees were not performing their work "*at least primarily, in the territory of another Member State*'". The NFT challenged this judgment and brought the case before the Dutch Supreme Court, which decided to stay the proceedings and refer the case to the CJEU for a preliminary ruling regarding a series of questions on when workers are posted "*to the territory of a Member State*" in the international road transport sector.

CJEU Ruling

First, the CJEU confirmed that operations of international road transport of goods fall in the scope of the Directive, as the Directive only excludes from its scope the services involving merchant navy seagoing personnel.

Second, the CJEU observed that, for a worker to be regarded as being posted "*to the territory of a Member State*", the performance of his or her work must have a sufficient connection with that territory. The existence of such a connection is determined based on an overall assessment of factors such as the nature of the activities carried out by the worker concerned in that territory, the degree of connection between the worker's activities and the territory of each Member State in which the worker operates, and the proportion represented by those activities in the entire transport service.

In this respect, the CJEU found that the mere fact that employees receive their instructions and/or start and finish their assignment in the Netherlands is not sufficient to consider the employees as posted workers sufficiently connected to the territory of that Member State. Moreover, the CJEU also stated that the existence of a group affiliation between undertakings that are parties to a contract for the hiring-out of workers does not, as such, determine the degree of connection between the performance of the work and the territory of a Member State to which those workers are sent. Therefore, the existence of such a group affiliation is not relevant to determine whether there is a posting of workers.

As regards the specific case of cabotage operations (*i.e.*, national carriage of goods for hire or reward carried out by non-resident hauliers on a temporary basis in a host Member State), to which the Directive applies, the CJEU clarified that those transport operations take place entirely within the territory of the host Member State. This implies that the performance of the drivers' work during such operations has a sufficient connection with that territory and that such drivers should, as a rule, be considered as posted workers. The CJEU added that the duration of cabotage operations is irrelevant to the determination whether there has been a posting. However, the CJEU noted that there is a possibility under the Directive available to the Member States not to apply specific provisions of the Directive as regards minimum rates of pay, when the length of the posting does not exceed one month.

Finally, the CJEU held that, if workers are posted, Member States must, under the Directive, ensure that the undertakings concerned guarantee workers posted to their territory a specific number of essential terms and conditions of employment laid down by collective agreements which have been declared universally applicable, namely those which must be observed by all undertakings in the geographical area and in the profession or industry concerned. The question of whether a collective agreement has been declared universally applicable must be assessed under applicable national law. The CJEU added that this definition also covers a collective labour agreement which was not declared universally applicable, but whose compliance is a precondition for exemption from another collective labour agreement which, for its part, was universally applicable and whose provisions are essentially identical to those of that other collective labour agreement.

LITIGATION

Draft Royal Decree Introduces Written Procedure as General Rule in Administrative Litigation Section of Council of State

On 4 December 2020, the Federal Council of Ministers adopted a draft Royal Decree "*amending Articles 26 and 84/1 of the Regent's Decision of 23 August 1948 establishing the procedure before the administrative litigation section of the Council of State*" with a view to introducing the written procedure at the administrative litigation section of the Council of State (*Ontwerp van Koninklijk Besluit tot wijziging van de artikelen 26 en 84/1 van het Besluit van de Regent van 23 augustus 1948 tot regeling van de rechtspleging voor de afdeling bestuursrechtspraak van de Raad van State / Projet d'Arrêté royal modifiant les articles 26 et 84/1 de l'Arrêté du Régent du 23 août 1948 déterminant la procédure devant la section du contentieux administratif du Conseil d'État* – the ***Draft Royal Decree***).

In the agreement establishing the Federal Government of 30 September 2020, the Federal Government announced that it would evaluate the procedural rules before the Council of State and, if necessary, revise them to accelerate proceedings and increase legal certainty. The Draft Royal Decree will introduce a permanent legal basis for handling cases without a public hearing on the basis of written submissions before the administrative litigation section of the Council of State. The new rule will apply to all cases unless a party objects and requests a public hearing.

The Draft Royal Decree thus confirms the practice which Royal Decree No. 12 of 21 April 2020 "*on the extension of the procedural time limits before the Council of State and the handling in writing of cases*" had provisionally introduced in the COVID-19 pandemic (*Koninklijk Besluit nr. 12 van 21 april 2020 met betrekking tot de verlenging van de termijnen van de rechtspleging voor de Raad van State en de schriftelijke behandeling van de zaken / Arrêté royal n° 12 du 21 avril 2020 concernant la prorogation des délais de procédure devant le Conseil d'Etat et la procédure écrite*).

The Draft Royal Decree was submitted for review to the section legislation of the Council of State.

Court of Justice of European Union Clarifies Rules on Jurisdiction over Abuse of Dominant Position Claims Resulting from Contractual Arrangements

On 24 November 2020, the Court of Justice of the European Union (***CJEU***) handed down a judgment in which it found that, when ruling on its jurisdiction to hear a dispute relating to an alleged abuse of a dominant position which results from a pre-existing contractual relationship, a national court should rely on the provisions governing tort in Regulation No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (the ***Brussels Ibis Regulation***) (CJEU, 24 November 2020, case C-59/19, *Wikingerhof v Booking.com*).

In 2009, Wikingerhof GmbH & Co. KG (***Wikingerhof***), a hotel located in Germany, concluded a standard contract with Booking.com BV (***Booking.com***), an accommodation booking platform registered in the Netherlands. That contract contained a clause according to which disputes arising from the contract would be heard by the courts of Amsterdam (the Netherlands).

In 2015, Wikingerhof brought an action before the German Regional Court of Kiel to object to several amendments which Booking.com had made to its general terms and conditions. Wikingerhof claimed that, due to Booking.com's strong position on the market, Booking.com had been able to impose contractual terms and conditions on Wikingerhof which allegedly amounted to an abuse of dominant position contrary to German competition law.

In a first judgment which was confirmed on appeal, the German Regional Court found that it lacked jurisdiction to hear the dispute given that the contract between the parties explicitly provided for the jurisdiction of the courts of Amsterdam. Wikingerhof then brought a further appeal to the German Federal Court of Justice arguing that German courts had jurisdiction pursuant to Article 7(2) of the Brussels Ibis Regulation since the subject-matter of the dispute involved tort law (specifically the abuse of a dominant position) and the competent court should therefore be the court of "*the place where the harmful event occurred* […]".

Uncertain as to the exact response to this issue, the German Federal Court of Justice referred the matter to the CJEU for a preliminary ruling.

The CJEU held that to decide whether a dispute between contracting parties constitutes a matter relating to a contract (within the meaning of Article 7(1) of the Brussels Ibis Regulation) or a matter relating to tort (within the meaning of Article 7(2) of the Brussels Ibis Regulation), the referring court must examine the obligation which is the cause of the action (para. 31). More specifically, the CJEU considered that the matter relates to a contract when the interpretation of that contract "*appears indispensable to establish the lawful or, on the contrary unlawful nature of the conduct complained of*" (para. 32). Conversely, if the claim is based on rules of liability in tort, namely a violation of obligations required by law, and if the analysis of the contract is not essential to assess the lawfulness of the conduct at hand, the action is a matter which is related to tort (para. 33).

In the case at hand, the CJEU found that the legal issue at the heart of the dispute was whether Booking.com had violated German competition law, which prohibits abuses of a dominant position. In that context, the CJEU held that it was not indispensable to interpret the contract concluded between the parties to determine the lawfulness of Booking.com's practices. The CJEU therefore concluded that the action brought by Wikingerhof constituted a matter relating to tort within the meaning of Article 7(2) of the Brussels Ibis Regulation and could thus be argued before the German courts.

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