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

Legal 500 2019

January 2021

VBB on Belgian Business Law

Highlights

COMPETITION LAW
Federal Parliament Adopts Bill Correcting Competition Rules
Page 3

DATA PROTECTION
Belgian Data Protection Authority Penalises Unlawful Use of Facebook Fan Page
Page 9

INSOLVENCY
End of Temporary Protection Measures for Enterprises Forced to Close Due to Covid-19 Restrictions
Page 11

INTELLECTUAL PROPERTY
"IT'S LIKE MILK BUT MADE FOR HUMANS": General Court Rules on Distinctive Character of Trade Mark
Page 12

LABOUR LAW
Birth Leave for Fathers or Co-parents Increased to 15 Days on 1 January 2021
Page 14

PUBLIC PROCUREMENT
Court of Justice of European Union Clarifies Application of Optional Exclusion Grounds and Right to Self-cleaning
Page 16

"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

COMPETITION LAW 3
DATA PROTECTION 4
INSOLVENCY 11
INTELLECTUAL PROPERTY 12
LABOUR LAW 14
PUBLIC PROCUREMENT 16

vbb@vbb.com
www.vbb.com

Table of contents

COMPETITION LAW 3

Federal Parliament Adopts Bill Correcting Competition Rules 3

DATA PROTECTION 4

Advocate General of Court of Justice of European Union Confirms That Belgian Data Protection Authority Can Initiate Court Proceedings 4

European Data Protection Board Adopts Guidelines on Examples Regarding Data Breach Notification 5

European Commission's draft Standard Contractual Clauses Jointly Commented on by European Data Protection Board and European Data Protection Supervisor 6

European Data Protection Board Updates Brexit Information Note 8

Commission Report on Status of National Implementation of Specific General Data Protection Regulation Provisions 8

Belgian Data Protection Authority Penalises Unlawful Use of Facebook Fan Page 9

INSOLVENCY 11

End of Temporary Protection Measures for Enterprises Forced to Close Due to Covid-19 Restrictions 11

INTELLECTUAL PROPERTY 12

"IT'S LIKE MILK BUT MADE FOR HUMANS": General Court Rules on Distinctive Character of Trade Mark 12

Advocate General Issues Opinion on Copyright Trolls 13

LABOUR LAW 14

Brexit: Immigration Status of UK Employees After 31 December 2020 14

Birth Leave for Fathers or Co-parents Increased to 15 Days on 1 January 2021 14

PUBLIC PROCUREMENT 16

Court of Justice of European Union Clarifies Application of Optional Exclusion Grounds and Right to Self-cleaning 16

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

COMPETITION LAW

Federal Parliament Adopts Bill Correcting Competition Rules

On 28 January 2021, the Chamber of Representatives of the federal Chamber of Representatives adopted, in plenary session, Bill 1515 of 16 September 2020 "on various provisions relating to the economy" (*Wetsontwerp houdende diverse bepalingen inzake Economie / Projet de loi portant dispositions diverses en matière d'Économie* - the ***Bill***).

As explained previously (*See, this Newsletter, Volume 2020, No. 9, p. 3*), the Bill includes technical corrections to Book IV of the Code of Economic Law (*Wetboek van Economisch Recht / Code de droit économique*) which contains the Belgian competition rules. In its current form, Book IV includes terminology errors and erroneous cross-references, some of which concern the provisions imposing fines for "gun jumping" infringements and for abuses of economic dependency.

The Bill also clarifies that a request to lift or to amend the conditions attached to a merger clearance decision of the Belgian Competition Authority (*Belgische Mededingingsautoriteit / Autorité belge de la Concurrence* - the ***BCA***) constitutes one of the exceptions to the principle of full jurisdiction of the Markets Court of the Brussels Court of Appeal (*Marktenhof / Cour des marchés* - the ***Markets Court***) in competition cases. The clarification had become necessary because of an amendment made to Book IV during the legislative reform of the competition rules that took place in May 2019 (*See, this Newsletter, Volume 2019, No. 5, p. 4*). In a judgment delivered on 23 October 2019 in the Kinepolis case, the Markets Court interpreted this amendment as meaning that the Markets Court had been given full jurisdiction to review merger conditions (*See, this Newsletter, Volume 2019, No. 10, p. 8*). Once the Bill becomes law, the Markets Court will only be allowed to determine whether the BCA's conditional merger clearance should be annulled. If an annulment takes place, the Markets Court will have to refer the case back to the BCA.

The Bill became law and was published in the Belgian Official Journal of 11 February 2021.

DATA PROTECTION

Advocate General of Court of Justice of European Union Confirms That Belgian Data Protection Authority Can Initiate Court Proceedings

On 13 January 2021, Advocate General (***AG***) Michal Bobek issued an Opinion in case C-645/19 on the roles of the lead data protection authority (***DPA***) and other national DPAs in the context of cross-border enforcement of the personal data protection rules (the ***Opinion***). His Opinion confirms that the application of the One-Stop-Shop mechanism laid down in the General Data Protection Regulation (***GDPR***) does not preclude DPAs from starting proceedings before national courts.

The Opinion follows an action brought by the Belgian DPA against several companies belonging to the Facebook Group (Facebook Inc., Facebook Ireland Ltd and Facebook Belgium BV) before the Dutch-language Court of First Instance, Brussels (*Nederlandstalige Rechtbank van Eerste Aanleg Brussel / Tribunal de première instance néerlandophone de Bruxelles*). The Belgian DPA requested that Facebook be ordered to stop placing cookies on the devices of internet users established on the Belgian territory without their consent and to cease collecting data in an allegedly excessive manner when users browse a web page on the Facebook.com domain or the website of a third party, including through Facebook social plugins and pixels.

On appeal, the scope of the proceedings was restricted to Facebook Belgium, as the Court of Appeal of Brussels (*Hof van Beroep te Brussel / Cour d'appel de Bruxelles*) considered that it had no jurisdiction over Facebook Inc. and Facebook Ireland Ltd. Facebook Belgium argued that in the light of the new One-Stop-Shop mechanism established by the GDPR, only the DPA of the State of the controllers' main establishment in the EU (the so-called "lead DPA") is competent to initiate judicial proceedings against Facebook for infringements of the GDPR that concern cross-border data processing. Consequently, it argued that only the Irish DPA, and not the Belgian DPA, would have competence to continue the proceedings at issue.

Against this background, the Court of Appeal of Brussels referred six questions for a preliminary ruling to the Court of Justice of the European Union (***CJEU***) aimed at clarifying whether the GDPR precludes a national DPA other than the lead DPA from initiating court proceedings in its Member State against infringements of the GDPR with respect to cross-border data processing.

In his Opinion, AG Bobek assessed the scope and functioning of the One-Stop-Shop mechanism of the GDPR. He found that a national DPA *is* entitled to initiate proceedings before a court of that State for an alleged infringement of the GDPR with respect to cross-border data processing, even when it is not the lead DPA, *provided* that it does so in the situations and according to the procedures set out in the GDPR.

The AG considered that the lead DPA has a general competence over cross-border processing. Nevertheless, he found that other DPAs can initiate proceedings before their national courts in the following specific situations:

1. If the national DPA acts outside the material scope of the GDPR (for instance, because no personal data is processed; the use of cookies may fall outside this material scope);

2. If the national DPA investigates cross-border data processing carried out by public authorities, in the public interest, in the exercise of official authority or by controllers not established in the EU;

3. In situations where, despite there being cross-border processing of personal data that falls within the scope of the GDPR, no supervisory authority is to act as lead DPA. There is no lead DPA regarding cross-border processing by controllers that have no establishment in the EU. Such controllers must deal with local supervisory authorities in every Member State they are active in;

4. If the national DPA adopts urgent measures. This can concern a situation in which the national DPA is faced with persistent passiveness of the lead DPA in charge;

5. If the national DPA intervenes following a decision of the lead DPA not to handle a case.

AG Bobek concluded that there is no general prohibition for national DPAs other than the lead authority to initiate proceedings before national judicial courts in the situations where this is permitted under the GDPR. On the contrary, he found that the GDPR specifically provides for or implies various situations in which they are empowered to do so. However, the general rule is still that the lead DPA should be acting in a case of cross-border infringement.

The Opinion of the AG Bobek can be read here. The CJEU is expected to deliver a judgment in the coming months.

European Data Protection Board Adopts Guidelines on Examples Regarding Data Breach Notification

On 18 January 2021, the European Data Protection Board (***EDPB***) published new guidance on how to handle data breaches. It did so in the form of "Examples regarding Data Breach Notification" (Guidelines 01/2021 on Examples regarding Data Breach Notification – the ***Guidelines***). The Guidelines discuss 18 examples of data breaches, explaining in each case whether the breach must be notified to supervisory authorities and/or to the data subjects concerned. In addition, the Guidelines contain useful recommendations on preventive measures and solutions to mitigate the impact of data breaches.

The Guidelines follow earlier general guidance on the topic issued by the Article 29 Working Party (WP29) (Guidelines on Personal data breach notification under Regulation 2016/679, WP 250 – a discussion of which is available here). The Guidelines complement the WP29 guidance and provide more practical advice based on the common experience of the national supervisory authorities of the EEA countries following the entry into force of the General data Protection Regulation (***GDPR***).

The GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

A breach can take many different forms and can have a range of significant adverse effects on individuals such as loss of control over personal data, limitation of rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, or loss of confidentiality of personal data protected by professional secrecy. One of the data controller's essential obligations is to evaluate these risks to data subjects' rights and freedoms and implement appropriate technical and organisational measures to address them.

Below is an overview of the categories of data breaches addressed in the Guidelines and the criteria on which the EDPB relies to determine whether the breach must be notified to the supervisory authority and/or the data subjects.

Ransomware

First, the Guidelines discuss four examples of ransomware attacks. The examples show that the requirement to notify depends on: (i) whether data can be restored swiftly from backups; (ii) whether data was exfiltrated during the attack; (iii) the nature of the data concerned; and (iv) additional risk mitigation measures.

As for most other categories of examples addressed in the Guidelines, the EDPB underlines the importance of adequate preparation based on both technical measures, such as up-to-date patches and updates to minimise the likelihood of ransomware attacks, and organisational measures, such as adequate procedures for addressing incidents in a timely manner. This is because ransomware attacks can expose pre-existing vulnerabilities caused by inadequate security. The decisional practice of supervisory authorities in the various Member States shows that firms can be fined for failing to have adequate security in place in cases where a data breach initially attracted the attention of the supervisory authority.

Data Exfiltration Attacks

Data exfiltration attacks include attacks that exploit vulnerabilities in the services offered to third parties over the internet. The Guidelines discuss the example of malicious code being submitted through an online job application form. The EDPB considers that the breach in that case gives rise to a high risk to natural persons' rights and freedoms and that the data subjects should be informed, and the relevant supervisory authority should be notified.

Internal Human Risk Source

The Guidelines also point out that many personal data breaches are caused by human error. Examples of such breaches include a former employee copying business data, or personal data sent to the wrong recipients.

In the case of unauthorised access by a former employee, the EDPB indicates that prompt legal action against former employees who steal data may be required to prevent the illegitimate use of the data. It also recommends including clear language prohibiting unauthorised access and copying of data in employment contracts. Moreover, when an employee signals his/her intention to quit, the company may consider withdrawing certain forms of access or implementing access logs so that unwanted access can be logged and flagged.

In the case of data that are erroneously sent to the wrong addressees, the factors determining whether this incident should be notified are the possibility of limiting the risk of breaches in confidentiality by immediate remedial action, as well as the quantity and the nature of the data.

Lost or Stolen Devices and Paper Documents

Having adequate security can avoid the need to notify lost or stolen devices to supervisory authorities. The Guidelines explain that the controller should take into consideration the circumstances of the processing operation such as the type of data stored on the device that was lost or stolen. Security measures, such as full encryption of the content of the device, access control, multi-factor authentication, remote wipe, etc., can tip the assessment in favour of non-notification.

Mispostal

Mispostal occurs when packages or documents are sent to the wrong consignee due to human error. In such cases, it is important to identify how the human error could have happened and how it can be prevented.

Whether notification is required depends on the number of recipients and the nature of the data. If the number of recipients is low, the message does not contain sensitive data and the controller immediately discovered the mistake and informs the recipients of the mistake and asks them to delete the list, a data breach is unlikely to result in a risk to the rights and freedoms of the data subjects.

By contrast, in another example, the number of affected individuals is high. The Guidelines indicate that even if the controller contacted all the recipients and asked them to delete the message and not use the information, it cannot force the recipients to do so, and consequently, it cannot be sufficiently certain that all recipients will comply with the request. In this example, the EDPB is of the opinion that the firm will be required to notify the supervisory authority and the concerned data subjects.

Other Cases – Social Engineering

Finally, the Guidelines discuss examples of social engineering and identity theft. They advise against using knowledge-based authentication for services provided over the telephone. Instead, they recommend the use of authentication that results in a high degree of confidence that the authenticated user is the intended person.

For each category of examples, the Guidelines set out a non-exhaustive list of "advisable measures", which include some preventive ideas as well as possible solutions in case of breaches.

The Guidelines are now open for public consultation until 2 March 2021 and can be found here.

European Commission's draft Standard Contractual Clauses Jointly Commented on by European Data Protection Board and European Data Protection Supervisor

On 18 January 2021, the European Data Protection Board (***EDPB***) and the European Data Protection Supervisor (***EDPS***) published their joint opinions on the draft implementing decisions of the European Commission (***Commission***) on standard contractual clauses (***SCCs***) which were published in November 2020 (*See, this Newsletter, Volume 2020, No. 11, p. 15*).

The joint opinions relate to two sets of SCCs: (i) the Commission's draft implementing decision on SCCs for the transfer of data to third countries under Article 46 of Regulation 679/2016 (the ***General Data Protection Regulation*** or ***GDPR***) (the ***Transfer SCCs***) and (ii) the Commission's draft implementing decision on SCCs for contracts

between controllers and processors under Article 28 of the GDPR (the ***Processor SCCs***). Each of the bodies' joint opinions include an annex containing annotated versions of the relevant draft SCCs with suggested changes and specific comments. The opinion on the Processor SCCs also contains an annex with suggested changes to the draft Commission decision.

Joint Opinion on Transfer SCCs

The SCCs adopted by the Commission are one of the appropriate safeguards provided for by Article 46 of the GDPR. They allow a data controller or data processor to transfer personal data to a third country that has not been recognised as providing an adequate level of protection for personal data.

The EDPB and EDPS welcome the new Transfer SCCs considering the important developments that have taken place in the digital economy since the current Transfer SCCs were adopted by the Commission. Moreover, the Commission's draft Transfer SCCs address concerns that were raised in the *Schrems II* ruling of the Court of Justice of the European Union (***CJEU***) (The implications of the *Schrems II* ruling can be studied here).

Overall, the EDPB and EDPS state that the Commission's draft Transfer SCCs present a reinforced level of protection for data subjects. They welcome the fact that the update of the current Transfer SCCs intends to: (i) better reflect the widespread use of new and more complex processing operations, often involving multiple data importers and data exporters in a changed digital economy; and (ii) provide for specific safeguards to address the effect of the laws of the third country of destination on the data importer's compliance with the clauses. This relates to the question of how to deal with binding requests from public authorities in the third country to disclose personal data transferred.

However, the EDPB and EDPS call on the Commission to clarify that there may still be situations where, despite the use of the new Transfer SCCs, ad-hoc supplementary measures will prove necessary to ensure that data subjects receive a level of protection essentially equivalent to that guaranteed within the EU. For this reason, the EDPB and EDPS stress that the new Transfer SCCs will have to be used along with the EDPB Recommendations on supplementary measures (*See* our article on the EDPB's Recommendations in *this Newsletter, Volume 2020, No. 11, p. 14*).

The EDPB and EDPS request the Commission to clarify that, in the absence of laws in the third country relating to public authorities' access to personal data, the parties should investigate the available information and assess whether applicable practices relating to the personal data transferred could prevent the data importer from fulfilling its contractual obligations under the SCCs.

Furthermore, the Joint Opinion calls on the Commission to provide further clarification in relation to the rights of data subjects under the Transfer SCCs, as well as the liability regime and possible interactions with Supervisory Authorities.

Joint Opinion on Processor SCCs

Pursuant to Article 28 of the GDPR any processing for which a controller relies on a processor (irrespective of whether the processor is located inside or outside the EU/EEA) "*shall be governed by a contract or other legal act* [...] *that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller*". In addition, the contract must address the elements listed in Articles 28.3 and 28.4 of the GDPR. Article 28.7 of the GDPR allows the Commission to adopt SCCs to comply with these requirements.

The EDPB and EDPS welcome the adoption of Processor SCCs under Article 28.7 as a strong accountability tool that facilitates compliance by controllers and processors with their obligations under the GDPR and Regulation 2018/1725 *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* (***EUDPR***). Overall, the aim is to ensure full harmonisation and legal certainty across the EU for contracts between controllers and their processors.

Nonetheless, the EDPB and EDPS consider that the Commission's draft Processor SCCs do not offer sufficient clarity. For instance, the Processor SCCs appear to cover only situations in which the controller and the processor are in the EU/EEA. The EDPB and the EDPS question why the Processor SCCs could not be used in other situations, for

instance if personal data are transferred to third countries that have been recognised as providing an adequate level of protection. Also, the Commission is requested to clarify the interplay between the Processor SCCs and the Transfer SCCs (discussed above).

In addition, the EDPB and EDPS suggest that where multiple entities are a party to the Processor SCCs, the SCCs should require the parties to detail and delimit the allocation of responsibilities and indicate clearly which processing is carried out by which processor(s) on behalf of which controller(s) and for which purposes. Additionally, the EDPB and EDPS would welcome clarification on how new parties can accede to the Processor SCCs (*i.e.*, whether consent by the contracting parties should be in writing, the deadline to provide such consent and the information needed before consent can be given).

The Joint Opinion on Transfer SCCs can be found here (and the Annex with the amended draft SCCs can be consulted here).

The Joint Opinion on Processor SCCs can be found here (while the Annexes with the amended draft Commission decision can be consulted here and the amended draft SCCs can be consulted here).

European Data Protection Board Updates Brexit Information Note

Following the adoption on 24 December 2020 of the EU-UK Trade and Cooperation Agreement (the ***EU-UK Trade Agreement***), the European Data Protection Board (***EDPB***) released on 13 January 2021 an updated version of its *Statement on the withdrawal of the UK from the European Union* (the ***Statement***) and its *Information note on data transfers under the GDPR to the UK after the transition period* (the ***Information Note***).

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 period, personal data can continue to be transferred from the EU to the UK even in the absence of additional safeguards. The EDPB's Information Note points out that, if no adequacy decision applicable to the UK as per Article 45 of the General Data Protection Regulation (the ***GDPR***) is adopted by 30 June 2021, all transfers of personal data between stakeholders subject to the GDPR and UK entities will constitute a transfer of personal data to a third country and will therefore be subject to Chapter V of the GDPR. Such transfers will require appropriate safeguards such as Standard Contractual Clauses (***SCCs***), Binding Corporate Rules (***BCRs***) or codes of conduct with enforceable data subject rights and effective legal remedies for data subjects.

In its Statement, the EDPB observes that the One-Stop-Shop mechanism of the GDPR ceased to apply to the UK on 1 January 2021. Moreover, controllers and processors not established in the EEA but whose processing activities are subject to the GDPR pursuant to its Article 3(3) are reminded of their obligation to designate a representative in the European Union in accordance with Article 27 of the GDPR.

The Statement is available here and the Information Note here.

Our Brexit Q&A can be found here.

Commission Report on Status of National Implementation of Specific General Data Protection Regulation Provisions

On 6 January 2021, the Directorate-General for Justice and Consumers of the European Commission issued a report on the implementation by the Member States of specific provisions of the General Data Protection Regulation (the ***GDPR***) (the ***Report***).

The Report discusses the implementation of GDPR provisions that allow Member States to determine conditions applicable to (i) obtaining valid consent from children in relation to information society services (Article 8(1) of the GDPR); (ii) limitations to the processing of special categories of personal data such as genetic data, biometric data or data concerning health (Article 9(4) of the GDPR); (iii) restrictions to the exercise of data subjects' rights if such restrictions respect the fundamental rights and are necessary and proportionate to safeguard public security and other important objectives of general public interest (Article 23(1)(c) and (e) of the GDPR); and (iv) national derogations from specific data subject rights for scientific or historical research, statistical, or public interest purposes (Article 89(2), (3) and (4) of the GDPR).

The Report analyses the legislation in the Member States to determine if the requirements imposed by the above provisions of the GDPR are adequately reflected in each Member State's legal framework. The Report summarises the assessments performed for all 27 EU Member States.

One general observation is that most Member States have set an age limit lower than 16 years of age for the validity of the consent of a minor in relation to information society services. The GDPR determines the age limit for minors to give valid consent in relation to such services at 16 years but Article 8(1) of the GDPR allows the Member States to establish a lower age limit (but not below the age of 13).

The Report notes that, with respect to Article 9(4) of the GDPR, most Member States impose additional rules on the processing of genetic data, biometric data or data concerning health. Many Member States limit access to such data or make the processing subject to prior authorisation from the competent national authority.

Finally, the Report calls for closer attention for two trends:

- First, most of the Member States implemented various restrictions on data subjects' rights under Articles 23(1)(c) and (e) and 23(2) of the GDPR for purposes of public security, public administration, public health, taxation, and migration. However, many Member States did not implement the conditions pursuant to Article 23(1) of the GDPR, which provides that such restrictions should respect the essence of the fundamental rights and freedoms and are a necessary and proportionate measure in a democratic society to safeguard;

- Second, for exemptions or derogations from Chapters II (principles); III (rights of the data subject); IV (controller and processor); V (transfer of personal data to third countries or international organisations); VI (independent supervisory authorities); VII (cooperation and consistency); and IX (specific data processing situations) of the GDPR for processing carried out for journalistic purposes or for the purpose of academic, artistic or literary expression as foreseen in Article 85(2) of the GDPR, only a handful of Member States made a case-by-case assessment of the exemptions/derogations to determine if these are necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information.

The full Report and its annexes can be consulted here.

Belgian Data Protection Authority Penalises Unlawful Use of Facebook Fan Page

On 12 January 2021, the Litigation Chamber (*Geschillenkamer/Chambre Contentieuse* – the ***Litigation Chamber***) of the Data Protection Authority (*Gegevensbeschermingsautoriteit/Autorité de protection des données* – the ***DPA***) imposed a fine of EUR 10,000 on a firm that made an unlawful continued use of an artist's Facebook fan page after the contract with the artist had ended.

Factual Background

The firm hosting the Facebook fan page (the ***firm***) and the artist (the ***claimant***) had a long contractual relationship until the agreement was terminated at the end of 2019. Following this termination, the claimant asked the firm several times to end the hosting of her fan page and to transfer her the rights to manage the page herself. As the firm did not comply with this request, the claimant filed a complaint with the DPA in March 2020.

In accordance with Article 95, §1, 4° and 5° of the Law establishing the Data Protection Authority (*Wet tot oprichting van de Gegevensbeschermingsautoriteit/Loi portant création de l'Autorité de protection des données*), the Litigation Chamber adopted a first decision on 14 April 2020 warning the firm regarding the unlawful data processing and urging it to comply with the claimant's request to exercise her rights under Articles 20 and 21 of the General Data Protection Regulation (***GDPR***) within seven days following the decision. The Litigation Chamber referred to this first decision as a so-called "light" decision. The firm appealed this decision to the Market Court in the Brussels Court of Appeal (the ***Court of Appeal***). This appeal did not prevent the Litigation Chamber from continuing the proceedings on the merits since it was clear that the firm would not comply with this first decision. The Court of Appeal overturned the Litigation Chamber's "light" decision in October 2020, but it did not rule on the merits.

In addition to the proceedings before the DPA, the claimant initiated proceedings before the Enterprise Court of Leuven (*Ondernemingsrechtbank/Tribunal de l'entreprise*) against the firm. In November 2020, the Enterprise Court found the firm guilty of unfair market practices on account

of the commercial use of the claimant's personality rights. The Enterprise Court did not address the violations of the GDPR.

Litigation Chamber's Decision on Merits

Because the firm continued hosting the Facebook fan page of the claimant after the contractual relationship had ended, the Litigation Chamber found the firm to be in breach of Article 6 of the GDPR. There was no longer a contractual relationship that could be invoked as legal ground for processing and there was also no consent from the claimant. The firm tried to rely on "legitimate interests" but the DPA did not follow that reasoning. The Litigation Chamber agreed that the claimant's reputation and success as an artist can have a certain impact on copyrights the firm would have and on the exploitation of certain rights of the firm. However, in this case, the processing went well beyond the mere use of the surname and first name of the claimant for the exploitation of works protected by copyright or of interest to the commercialisation of the firm's artistic projects. Given the close connection of the claimant's person with the fan page, the Litigation Chamber considered that the claimant, as a data subject, should receive the hosting rights of the page to manage her own personal data. The Litigation Chamber also referred to Article 8 of the Charter on Human Rights which protects a person's identity as a fundamental right.

Furthermore, the firm infringed Article 21(1) of the GDPR because it had failed to comply with the claimant's request to stop the data processing. The Litigation Chamber specified that the firm should have complied with this request immediately even if it had assumed that it had legitimate interests because these did not outweigh the rights, interests, and freedoms of the claimant.

Moreover, as a controller, the firm should have informed the data subject of the reasons for not acting following its request and had to inform the data subject of the possibility to lodge a complaint with a supervisory authority and to seek judicial remedy. The firm's failure to do so constituted a further infringement of the GDPR.

For these reasons, the Litigation Chamber imposed a fine of EUR 10,000 on the firm for breach of Articles 6, 21(1) and 12(3) of the GDPR. In determining the amount of the fine, the Litigation Chamber considered that the infringed provisions belong to the core of the GDPR that relate to the lawfulness of processing and rights of data subjects. The Litigation Chamber also considered it unacceptable that the commercial interests of the firm would in any way harm the rights of the claimant under Articles 12 to 22 of the GDPR. The fine had to have a deterrent effect because the firm had made an incorrect assessment of the importance of its own commercial interests compared to the claimant's personal data protection rights.

The DPA decision is currently only available in Dutch here.

INSOLVENCY

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

On 31 January 2021, the protection measures for enterprises forced to close because of the restrictions imposed in the Covid-19 crisis ended. These protection measures formed part of the Law of 20 December 2020 containing various temporary and structural provisions regarding justice within the context of 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 had established a statutory moratorium from 24 December 2020 until 31 January 2021 for enterprises that had been forced to close down pursuant to the Ministerial Decree of 1 November 2020 setting out emergency measures to limit the spread of the Covid-19 (the ***Moratorium***) (*See, this Newsletter, Volume 2020, No. 12, p. 13*). Under the Moratorium, these enterprises were protected against (i) bankruptcy and judicial dissolution; (ii) attachment and enforcement measures; and (iii) termination of contracts because of failure to pay.

Because these protection measures have not been extended, businesses are now again exposed against claims for bankruptcy and attempts by creditors to seize their assets.

A new law is expected to be adopted by March 2021 that will simplify the judicial reorganisation procedure in several respects, for example by easing the formal conditions to open such a procedure and extending the situations in which a judicial officer can be appointed.

INTELLECTUAL PROPERTY

"IT'S LIKE MILK BUT MADE FOR HUMANS": General Court Rules on Distinctive Character of Trade Mark

On 20 January 2021, the General Court of the European Union (***GC***) allowed the registration of the trade mark "IT'S LIKE MILK BUT MADE FOR HUMANS" in case T-253/20 *Oatly AB v EUIPO*. The GC confirmed that the distinctiveness test for trade mark registration consists in determining whether the relevant public is capable of distinguishing the applicant's goods from goods which have another commercial origin. If this is the case, the mark meets the requirement of having the minimum distinctive character and qualifies for registration under Article 7(1)(b) of Regulation 2017/1001 on the European Union Trade Mark (***Regulation 2017/1001***). The GC thus overturned the decision of the European Union Intellectual Property Office (***EUIPO***) which had denied trade mark registration.

Factual Background and Procedure

On 14 March 2018, Oatly AB filed an application for registration for an EU trade mark with the EUIPO for the word sign "IT'S LIKE MILK BUT MADE FOR HUMANS". The registration was sought in the following classes of goods: 18 (including leather products), 25 (including footwear and headwear), 29 (including dairy substitutes), 30 (including foodstuff of plant origins) and 32 (including beverages). The EUIPO objected to the registration for classes 29, 30 and 32 on the ground that the word sign lacked the distinctive character required by Article 7(1)(b) of Regulation 2017/1001. After Oatly AB submitted its observations, the examiner issued a refusal to register the goods in Classes 29 (dairy substitutes), 30 (oat-based food) and 32 (beverages). .

On 30 October 2019, Oatly filed an appeal with the Board of Appeal of EUIPO (***Board of Appeal***) which was dismissed on 7 February 2020. The Board of Appeal held that it would consider the perception of the English-speaking public in the European Union (***EU***). The Board's reasoning was that the slogan had a first component "IT'S LIKE MILK" referring to a milk substitute, and a second component "BUT MADE FOR HUMANS", implying that it was better suited for human consumption than other milk-related products. The Board thus held that the slogan did not have the distinctive character required by Article 7(1)(b) of Regulation 2017/1001 to register a trade mark.

GC's Reasoning

Oatly AB appealed the decision to the GC, alleging that the Board of Appeal incorrectly assessed the relevant public and the distinctive character of the trade mark applied for. The General Court relied on its established case-law concerning the distinctive test of Article 7(1)(b) of Regulation 2017/1001, as expressed in case C-398/08 P *Audi v. OHIM*. In that case, the Court held that the distinctive character of a trade mark must be assessed by reference to (i) the goods or services for which the registration has been applied for; and (ii) the relevant public's perception of the mark. Even a minimum degree of distinctiveness suffices to avoid refusal of the registration. In addition to the indication of origin, it must be borne in mind that a mark can also fulfil other functions such as advertising slogans or quality indication.

Regarding the definition of the relevant public, the GC accepted Oatly's argument that the English-speaking part of the EU does not only consist of the countries in which English is the official language. Member States such as Denmark, Finland, the Netherlands, and Sweden where English is widely understood should be considered as well.

Regarding the distinctive character of the trade mark, the Board of Appeal had considered the slogan to be promotional in the ongoing milk consumption debate rather than an indication of the goods' commercial origin as it would indicate a better suitability for human consumption than other types of milk. By contrast, the GC agreed with Oatly AB's counterargument that the relevant public is made up of average consumers without extreme or minority opinions and are buyers of everyday consumer goods. With this slogan, Oatly AB challenges the public's preconception that milk is an essential part of the human's diet. As proof, Oatly AB pointed at the controversies that its launching campaign created in the Netherlands, Sweden, and the United Kingdom.

The GC concluded that the Board of Appeal mistakenly rejected the registration of the trade mark and that the sign met the distinctive character requirement within the meaning of Article 7(1)(b) of Regulation 2017/1001.

Advocate General Issues Opinion on Copyright Trolls

On 18 December 2020, Advocate General Szpunar (AG) issued an opinion regarding the concept of "communication to the public" in case C-597/19 *Mircom International Content Management & Consulting (MICM) Limited v Telenet BVBA*. The case involved "copyright trolls": entities that obtain limited rights to exploit copyrights from the holders and rely on those rights to threaten users on peer-to-peer sharing platforms with lawsuits to collect compensation which often exceeds the actual damage suffered. According to the AG, copyright trolls should not obtain information about the users who share copyright-protected content because this would amount to a fraudulent use of EU Law. In addition, the AG held that "seeding", which is the sharing of files containing protected content through BitTorrent technology, constituted 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***).

Mircom, the claimant in this procedure, is a company incorporated under Cypriot law. It holds licenses with producers of erotic films established in the United States and Canada for the communication to the public of their films on peer-to-peer networks, especially in Europe. Mircom investigates acts of infringements of producers' rights committed on such networks. It brought an action before the Antwerp Enterprise Court (the ***Court***) to obtain from Telenet and several other internet providers, the identification data from their customers who had shared films from Mircom by means of BitTorrent.

The Court referred four questions to the Court of Justice of the European Union (***CJEU***) for a preliminary ruling. First, the Court sought to know whether uploading files or parts of it could be regarded as a communication to the public within the meaning of Article 3(1) of the Infosoc Directive. In case of a positive answer, the Court also asked if there is a *de minimis rule* and whether the user should have actual knowledge of the seeding (which is not always the case since this happens automatically). Second, the Court asked whether the rightholders who do not exploit their rights are entitled to the same protection under Directive 2004/48 on the Enforcement of Intellectual Property rights (***Enforcement Directive***) as the rightholders who do exploit their rights and, if so, how they can suffer prejudice because of an infringement. In its third question, the Antwerp court sought guidance from the CJEU on how to strike a balance between the fundamental rights that are at stake in the first two questions. Finally, the CJEU was asked whether Mircom's registration and general processing of data complies with the General Data Protection Regulation (***GDPR***).

On the first question, the AG confirmed that Article 3 of the Infosoc Directive should be interpreted as meaning that uploading pieces of a file containing protected work on a peer-to-peer network amounts to making work available to the public. The AG is of the opinion that it does not matter whether the user has full knowledge of this practice. For both seeders (users who have the complete file and share it by uploading it) and peers (users who download and upload the files) there is no need to apply a threshold to determine whether there is a communication to the public since it does not matter whether the transmission actually occurs as long as the user makes it possible. For leechers (user who download the files from the torrent link) it is sufficient that the protected works have been downloaded on a peer-to-peer network.

Second, the AG held that Article 4(b) of the Enforcement Directive must be interpreted in the sense that a body having acquired certain rights for the sole purpose of claiming damages and not to exploit these rights, should not benefit from the remedies of Chapter 2 of that Directive.

Third, Articles 8(1) and 3(2) of the Enforcement Directive should be interpreted as meaning that the national court must refuse to grant the right of information requested, as this demand is unjustified or unlawful.

Fourth, the AG is of the opinion that the recording of the IP addresses of the persons whose internet connections were used to share protected work on peer-to-peer network constitutes a lawful processing of personal data under Article 6 of the GDPR as it is carried out in a legitimate interest of the controller or third party.

The opinion of the AG is not binding on the CJEU which is expected to deliver a judgment later this year.

LABOUR LAW

Brexit: Immigration Status of UK Employees After 31 December 2020

Background

Following the UK's departure from the European Union on 1 January 2021, UK nationals no longer benefit from the European principle of free movement for workers. This implies that as from 1 January 2021 Belgian employers should apply for a single permit (which covers both the work and residence permit of their employees) when employing UK nationals in Belgium longer than 90 days.

Law of 16 December 2020

However, the Law of 16 December 2020 on the beneficiaries of the agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (*Wet betreffende de begunstigden van het akkoord inzake de terugtrekking van het Verenigd Koninkrijk van Groot Brittannië en Noord-Ierland uit de Europese Unie en de Europese Gemeenschap voor Atoomenergie / Loi relative aux bénéficiaires de l'accord sur le retrait du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord de l'Union européenne et de la Communauté européenne de l'énergie atomique* - the ***Law***) provides for exceptions to this rule. The Law implements the immigration aspects of the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (the ***Withdrawal Agreement*** - for the full agreement, click here).

The Law and the Withdrawal Agreement safeguard the right of residence and the right to work in Belgium of UK employees and UK self-employed contractors if these persons exercised their right of free movement before 1 January 2021.

UK employees who were employed and had legal residency in Belgium before 1 January 2021 keep their right of residency and right to work in Belgium if they apply for an "M-card" with their municipality of residence before 31 December 2021. Frontier workers who live in the UK but regularly commuted for work to Belgium before 1 January 2021 benefit from a similar status and should apply for a frontier worker "N-card" with the municipality where they work before 31 December 2021.

Birth Leave for Fathers or Co-parents Increased to 15 Days on 1 January 2021

Pursuant to the Programme Law of 20 December 2020 (*Programmawet / Loi-programme*) which modifies the Law of 3 July 1978 on employment contracts (*Wet betreffende de arbeidsovereenkomsten / Loi relative aux contrats de travail*), birth leave for fathers or co-parents (as it is a gender-neutral type of paternity leave) will increase from ten working days to 15 working days, as from 1 January 2021.

Employees will be able to schedule their leave days within four months following the childbirth. The 15 days can be taken separately or in a row. They can also be split up in up to 30 half-days.

Pursuant to the Programme Law, the leave will increase further with an additional five working days, to a total of 20 working days on 1 January 2023.

During the first three days of birth leave, the employees will be entitled to their normal salary. For the remaining days, they will enjoy a benefit allowance of 82% of their (capped) salary which is paid by the Belgian health insurance authorities.

The birth leave merely constitutes a right of the employees, but it is not mandatory to take such leave (or the maximum number of days as provided for by the Programme Law).

Employees who wish to benefit from birth leave should inform their employer in advance in writing. From the day of this written notification, the employees will be protected against dismissal for a period of three months. This implies that the employer must not terminate the employ-

ee's employment contract, except for reasons unrelated to the birth leave.

If this rule is not observed, a protection indemnity of three months' gross salary will be due by the employer in addition to the normal severance pay.

PUBLIC PROCUREMENT

Court of Justice of European Union Clarifies Application of Optional Exclusion Grounds and Right to Self-cleaning

On 14 January 2021, the Court of Justice of the European Union (***CJEU***) held that tenderers who find themselves in one of the optional grounds for exclusion referred to in Article 57(4) of Directive 2014/24/EU of 26 February 2014 on public procurement (the ***Directive***) are only obliged to demonstrate spontaneously that the corrective measures which they took are sufficient to demonstrate their reliability despite the existence of an exclusion ground, if this is required by national law or specified in the tender documents. The CJEU added that Article 57(6) of the Directive has direct effect (CJEU, judgment of 14 January 2021, Case C-387/19, *RTS Infra and Aannemingsbedrijf Norré-Behaegel*).

Article 57(6), first paragraph of the Directive provides for the right to "*self-cleaning*". It allows tenderers who fall within the ambit of an optional ground for exclusion to "*provide evidence to the effect that measures taken by* [them] *are sufficient to demonstrate* [their] *reliability despite the existence of a relevant ground for exclusion*". The provision continues that "[i]*f such evidence is considered as sufficient, the economic operator concerned shall not be excluded from the procurement procedure*". The subsequent paragraphs describe the burden of proof that rests on the economic operator and the evaluation criteria to be applied by the contracting authority.

The CJEU delivered its judgment in response to a question referred to it for a preliminary ruling by the Belgian Council of State (*Raad van State / Conseil d'État*) in a dispute between two road construction companies, RTS Infra BV and Aannemingsbedrijf Norré-Behaegel BV (the ***Applicants***), and the Flemish Region. In a public procurement procedure, the Flemish Region had excluded the Applicants from participating in the procedure and had thus disregarded their tenders and awarded the contract to the bidder with the lowest regular tender. The Flemish Region had justified its decision to exclude the Applicants by the fact that they had been guilty of "*serious professional misconduct*" in performing previous contracts awarded by the Flemish Region. According to that body, the serious and repeated contractual shortcomings of the Applicants in past contracts created doubt and uncertainty as to their ability to carry out the new contract in a correct manner.

The Applicants requested the Council of State to annul the Flemish Region's exclusion decision. They argued that, before being excluded on account of the alleged serious professional misconduct, they should have been given the opportunity to defend themselves and to demonstrate that they had remedied the consequences of that misconduct by taking appropriate corrective measures, as provided for in Article 57(6) of the Directive, which they claimed has direct effect. The Flemish Region challenged that position and referred to Article 70 of the Law of 17 June 2016 on public procurement (*Wet van 17 juni 2016 inzake overheidsopdrachten / Loi du 17 juin 2016 relative aux marchés publics* – the ***Law***). While admitting that Article 70 had not yet entered into force at the time of the facts of the case, the Flemish Region noted that this provision requires economic operators to indicate the corrective measures taken of their own motion.

The Council of State sought guidance from the CJEU as to whether:

1. Article 57(6) of the Directive precludes EU Member States from requiring economic operators, when submitting their request to participate or their tender in a public procurement procedure, to provide, spontaneously, evidence of the corrective measures which they took to show their reliability despite the existence of an optional ground for exclusion referred to in Article 57(4) of the Directive, if no such obligation arises from the applicable national legislation or the tender documents; and

2. Article 57(6) of the Directive has direct effect.

As regards the first question, the CJEU started by noting that, in the absence of any stipulations to the contrary in the Directive and in view of its goals, Article 57(6) of

the Directive must necessarily be interpreted as allowing economic operators to furnish evidence of the corrective measures taken both of their own initiative and on that of the contracting authority, and both when submitting their tender or the request to participate in the procurement procedure and at a later stage of the procedure.

Referring to (i) the principles of procurement, including the principles of non-discrimination, transparency and proportionality; and (ii) the general principle of respect for the rights of the defence, the CJEU continued that, in view of Article 57(6) of the Directive, the Applicants could reasonably expect the Flemish Region to give them the opportunity to demonstrate that the corrective measures which they had taken were sufficient to remedy the optional grounds for exclusion invoked by the Flemish Region. The CJEU added that is true that the principles of transparency and loyalty required the applicants to include in their tender documentation information on their serious professional misconduct in the performance of past contracts awarded by the same contracting authority. However, this duty of the applicants could not exempt the Flemish Region from its obligation to give the Applicants the opportunity to provide evidence of the corrective measures taken.

In response to the second question, the CJEU confirmed that Article 57(6) of the Directive has direct effect and can be invoked directly by the Applicants. Even though Article 57(6) leaves the EU Member States a degree of latitude when adopting further procedural rules, the provision affords economic operators a minimum level of protection. Moreover, Article 57(6) of the Directive lays down the basic elements of the "*self-cleaning*" scheme and the associated economic operator's rights in that the provision clarifies what must be proved as a minimum and which evaluation criteria must be applied.

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