"Van Bael & Bellis' 'responsive and knowledgeable team' gives very good advice, both at EU and domestic level."

Legal 500 2017

November 2019

VBB on Belgian Business Law

Highlights

Renowned competition and trade boutique which continues to gain visibility in M&A and private equity transactions, with strong cross-border capabilities, earning praise for its commitment and management of global transactions.

Chambers Europe 2017

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

CAPITAL MARKETS AND FINANCIAL LAW

FSMA Implements ESMA Guidelines on Risk Factors Under Prospectus Regulation

On 12 November 2019, the Belgian Financial Services and Markets Authority (*Autoriteit voor Financiële Diensten en Markten / Autorité des services et marchés financiers;* ***FSMA***) announced that it would comply with the Guidelines on risk factors under the Prospectus Regulation (the ***Guidelines***) which were issued by the European Securities and Markets Authorities (***ESMA***) on 1 October 2019.

The Guidelines seek to effect a more focused and streamlined disclosure of risk factors, in an easily analysable, concise and comprehensible form. They include twelve recommendations assisting the competent authorities in their review of the specificity, materiality and presentation of the risk factors.

The Guidelines are addressed to the FSMA as the competent authority to apply the Prospectus Regulation. However, they should also be taken into account by the parties responsible for preparing the prospectus for submission to the FSMA in order to facilitate the approval process.

The Guidelines have been applied by the FSMA since 4 December 2019 and can be found here.

COMPETITION LAW

Commission Approves State Aid to Airports of Antwerp and Ostend-Bruges

On 12 November 2019, the European Commission (the ***Commission***) announced that it had approved state aid for the benefit of the airports of Antwerp and Ostend-Bruges.

Belgium wishes to grant approximately EUR 12 million to the airport of Antwerp in operating aid and investment aid for the modernisation of its safety infrastructure. On the basis of its Guidelines on State aid to airports and airlines, the Commission concluded that the aid would increase the accessibility of Antwerp, stimulate its growth and that of the Flemish Region and increase the mobility of EU citizens, without affecting competition in the internal market.

In addition, the Commission reviewed operating aid of EUR 2.3 million that Belgium had granted to the airport of Ostend-Bruges. Following a similar review, the Commission held that the aid would also stimulate the development of the Flemish Region without affecting competition in the internal market.

The Commission press release is available in Dutch, French and German.

Telenet Challenges Mobile Network Sharing of Orange Belgium and Proximus

On 22 November 2019, Proximus published a press release confirming that it had signed an agreement with Orange Belgium to set up a shared mobile access network. That network would be operated by a 50/50 joint venture company between Orange Belgium and Proximus. The network sharing would result in significant cost savings for both telecommunications network operators. This is a path which other operators of mobile communications networks elsewhere in the EU have also followed in an attempt to deal with infrastructure investments, including the finance required to roll out new 5G networks. Proximus and Orange Belgium maintain that they will continue to compete independently at the retail and wholesale levels. They claim that they will also be rivals in acquiring 5G spectrum.

While Telenet, a competing telecommunications operator, reportedly initially participated in talks to join the network sharing agreement, it later withdrew from the talks and has now filed a complaint with the Belgian Competition Authority (the ***BCA***) to challenge and have the implementation of the network sharing agreement suspended. The BCA is expected to hand down a decision regarding Telenet's request by early 2020.

For its part, in August 2019, the European Commission has already issued a statement of objections against an ostensibly less far-reaching network sharing arrangement in the Czech Republic.

CONSUMER LAW

Council of European Union Adopts Directive on Better Enforcement and Modernisation of EU Consumer Protection Rules

On 8 November 2019, the Council of the European Union (the ***Council***) adopted a proposal for a Directive amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU as regards the better enforcement and modernisation of Union consumer protection rules (the ***Directive***). The proposal had been published by the European Commission on 11 April 2018 and was adopted by the European Parliament on 17 April 2019.

The Directive, which was adopted as part of the "New Deal for Consumers" package (See, this Newsletter, Volume 2018, No. 4, p. 7), focuses on five aspects of consumer protection: (i) penalties for widespread infringements, including cross-border infringements; (ii) transparency of online marketplaces; (iii) protection for consumers of 'free' digital services; (iv) dual quality products; and (v) the consumers' right of withdrawal from contracts for the supply of digital content or digital services.

Widespread Infringements

First, the Directive aims to correct the lack of uniformity in EU Member States' rules on penalties for "*widespread infringements*" and "*widespread infringements with a Union dimension*" of Union laws that protect consumers' interests, within the meaning of Article 2 of Regulation (EU) 2017/2394 on cooperation between national authorities responsible for the enforcement of consumer protection laws. Such infringements encompass practices which harm large numbers of EU consumers. The Directive harmonises some of the criteria used to determine the level of penalties for infringements of the Directives which it amends. Fines for such infringements will amount to at least four percent of the trader's annual turnover in the EU Member State(s) concerned.

Transparency of Online Marketplaces

Second, the Directive introduces additional transparency requirements for online marketplaces. These must inform consumers about: (i) the identity of their contractual counterpart and of the trader (*i.e.,* a third-party supplier or the online marketplace), which is responsible for guaranteeing consumer rights related to the contract; (ii) the parameters determining the ranking of different offers; and (iii) whether consumer protection legislation applies.

Free Digital Services

Third, the Directive extends the scope of application of Directive 2011/83/EU on consumer rights (the ***Consumer Rights Directive***) to 'free' digital services, such as cloud storage, social media and e-mail accounts, for which consumers tender personal data instead of monetary compensation. As a result, consumers of such digital services will also benefit from basic rights, such as the pre-contractual information required by the Consumer Rights Directive and the 14-day cooling-off period (or "right of withdrawal").

Dual Quality Products

Fourth, the Directive provides clarifications on the way misleading marketing of dual quality products should be tackled by EU Member States. The issue of the dual quality of branded products may arise if products are sold in various EU Member States with the same or a similar brand name and packaging but, in reality, differ in their composition or characteristics from one EU Member State to the other in a way that may mislead consumers and cause them to take a transactional decision that they would not have otherwise taken.

Right of Withdrawal

Finally, the Directive clarifies traders' and consumers' rights in case consumers exercise their right of withdrawal from a contract for the supply of digital content or digital services. The difference between the supply of digital content and the provision of digital services lies in the continuous nature of the latter. The right of withdrawal allows a consumer to test a service and decide, over a 14-day period as of the conclusion of the contract, whether to keep using

the service or not. Contracts for the supply of digital content not supplied on a tangible medium are currently subject to an exception from the right of withdrawal pursuant to Article 16 of the Consumer Rights Directive. Accordingly, a consumer loses the right of withdrawal when the performance of the contract is started (*e.g.*, through downloading or streaming of the content). The Directive provides that, if there is doubt as to whether the contract is a service contract or a contract for the supply of digital content not supplied on a tangible medium, the rules on the right of withdrawal for services should apply.

The Directive will enter into force 20 days after its publication in the Official Journal of the EU. EU Member States will have until 27 November 2021 to implement its provisions in their national laws. National implementing provisions must become applicable by 27 May 2022.

CORPORATE LAW

Corporate Digitisation: Establishment of Database for Articles of Association and Digital Share Register Platform

The new Belgian Companies and Associations' Code (***BCAC***) entered into force on 1 May 2019. One of the key goals of the BCAC is the digitisation of corporate housekeeping for companies and associations in Belgium.

Database for Articles of Association

The Federation of Notaries (***FedNot***) launched a new online database for articles of association. The database contains the most recent coordinated version of a company's articles of association, provided these date from 1 May 2019 or later. The coordinated articles of association that have been adopted prior to 1 May 2019 can still be consulted at the clerk's office of the competent enterprise court.

The database is publicly accessible, free of charge and can be consulted here.

Digital Share Registers

Furthermore, Fednot and the Belgian Institute for Tax Advisors and Accountants launched eStox, an online application for digital share registers.

The digital share register would replace the paper share register, which is now a physical book that is kept at the registered office of the company. The digitisation of the share register should make it easier for companies and their shareholders to keep the share register up to date and avoid data loss. Additionally, it will result in more consistency in the way information is recorded in share registers.

Finally, the digital share register platform eStox is linked to the Ultimate Beneficial Owner Register. This means that the relevant information regarding the ultimate beneficial owner of the legal entity can automatically be submitted to the Ultimate Beneficial Owner Register, facilitating compliance with the annual obligation to keep the information in this Register up to date.

At this stage, the eStox platform is only accessible to notaries, accountants and tax consultants. However, over time, the directors of companies will also obtain access to the register and be able to download digital copies of the share register.

DATA PROTECTION

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

On 13 November 2019, the European Data Protection Board (***EDPB***) published draft guidelines (the ***Guidelines***) on the principle of "Data Protection by Design and by Default" set out under Article 25 of the General Data Protection Regulation (***GDPR***). The Guidelines explain how controllers must ensure that they implement the "*data protection principles and data subjects' rights and freedoms by design and by default*" during the design and life cycle of processing activities.

The EDPB underlines that Data Protection by Design and Default is a requirement for all controllers, independent of their size. The examples contained in the Guidelines illustrate the broad range of processing activities to which this principle applies: from setting up membership administration to buying customer relationship management (CRM) software; designing online order forms; improving effectiveness of deliveries (through tracking employees); deciding on loan applications as a financial institution; or using artificial intelligence to profile customers. However, the complexity of implementing this principle will vary based on the individual processing operation. In this regard, the principle of Data Protection by Design and Default is coherent with the "risk-based approach" underlying the GDPR.

Data Protection by Design

Under the principle of "Data Protection by Design", data controllers are obliged to implement "appropriate technical and organisational measures" and "necessary safeguards" to implement data protection principles, such as lawfulness and data minimisation, and to protect the rights and freedoms of data subjects. The Guidelines explain these measures and safeguards and list elements that must be considered to determine which measures are "appropriate" or which safeguards are "necessary".

The EDPB clarifies that measures and safeguards must be implemented both at the time of determining the means of processing data and at the time of processing the data itself. A regular review of the effectiveness of the chosen measures and safeguards is required in order to ensure effective data protection at the time of processing.

The Guidelines furthermore explain that there is no requirement as to the sophistication of a technical or organisational measure as long as it is appropriate for implementing the data protection principles effectively. Such a measure can be anything, from the use of advanced technical solutions to the basic training of personnel (*e.g.,* on how to handle customer data). Necessary safeguards are, for example, enabling data subjects to intervene in the processing, providing automatic and repeated information about what personal data is being stored, or having a retention reminder in a data repository.

The *effective* implementation of the data protection principles means that controllers must be able to demonstrate that they implemented dedicated measures to protect these principles and that specific necessary safeguards were put in place. This compliance may be demonstrated by appropriate key performance indicators. Alternatively, controllers may provide the rationale for their assessment of the effectiveness of the chosen measures and safeguards.

Article 25 of the GDPR lists some elements which the controller has to take into account when determining the appropriate technical and organisational measures of a specific processing operation:

- The concept of "*state of the art*" imposes an obligation on controllers to take account of the current progress in technology that is available in the market. This means that controllers must have knowledge of and stay up to date on: (i) technological advances; (ii) how technology can present data protection risks to the processing operation; and (iii) how to implement the measures and safeguards that secure effective implementation of the principles and rights of data subjects. Taking into account technological advancements, a controller could find that a measure that once provided an adequate level of protection no longer does so. Existing standards and certifications may play a role in indicating the current "state of the art" within a field.

- The controller must consider the "*cost of implementation*" under the design process meaning that the costs necessary for the effective implementation of all the principles should be planned. In doing so, the controller may assess the risks to the rights and freedoms of data subjects that the processing entails and estimate the cost of implementing the appropriate measures into the processing to mitigate such risks to a level where the principles are effectively implemented. According to the Guidelines, spending more on technology does not necessarily lead to more effective implementation of the principles. In some instances, simple low-cost solutions can be more effective than costly counterparts.

- Controllers must take into consideration factors such as the "*nature, scope, context and purpose*" of processing.

- Article 25 of the GDPR obliges controllers to take account of "*risks of varying likelihood and severity for rights and freedoms of natural persons*" posed by the processing. Controllers must therefore always carry out an assessment of data protection risks for the processing activity at hand and verify the effectiveness of the measures and safeguards proposed.

Data Protection by Default

In addition, Article 25 of the GDPR requires "Data Protection by Default", which means that, by default, only personal data that are necessary for each specific purpose of the processing can be processed. This principle refers to the choices made by a controller regarding any pre-existing configuration value or processing option that is assigned in a software application, computer programme or device that has the effect of adjusting the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. Default settings must thus be designed with data protection in mind. Key aspects of the Guidelines relating to this principle are the following:

- If there were no default settings, data subjects would be overwhelmed by options that he or she may not have the ability to grasp. Thus, in many cases, controllers must decide on these options on behalf of the data subjects and must ensure that only the personal data that is necessary to achieve the purpose of the processing is enabled.

- Technical and organisational measures in the context of data protection by default is understood in the same way as explained above under the principle of "Data Protection by Design" but is applied specifically to the principle of data minimisation. The measures must, by default, be appropriate to ensure that only personal data which are necessary for each specific purpose of processing are being processed.

Implementation of Basic Data Protection Principles

The EDPB explains that Data Protection by Design and Default is a critical step to implement the data protection principles in Article 5(1) of the GDPR, such as transparency, lawfulness of processing and purpose limitation. The Guidelines offer practical guidance by listing key design and default elements as well as practical cases for illustration.

For instance, to illustrate how to implement the principle of "transparency" by design and by default, the Guidelines explain that, in general, providing a privacy policy on the website alone is not enough for the controller to meet the requirements of transparency. Data subjects should be able to understand, and if necessary, make use of their rights in Articles 15 to 22 of the GDPR. The controller can therefore design a privacy policy, but the necessary information must be provided in the right context and at the appropriate time. This implies that the controller should inform the data subject, when asking him/her to enter personal data, of how the personal data will be processed and why these personal data are necessary for the processing.

The Guidelines also address the possibilities of certification in accordance with Article 42 of the GDPR and supervisory authorities' enforcement of Article 25 of the GDPR. Finally, the EDPB provides recommendations on how controllers, processors and technology providers can cooperate to achieve "Data Protection by Design and by Default" and how they can turn this into a competitive advantage.

A copy of the EDPB's Guidelines can be found here. Stakeholders can submit comments on the draft until 16 January 2020.

Annual Review Confirms Validity of EU-US Privacy Shield

On 23 October 2019, the European Commission (***Commission***) published its report on the Third Annual Joint Review of the EU-US Privacy Shield. The Privacy Shield is a self-certification scheme whereby certified US organisations can more easily receive personal data transferred to them from the EU. Certification is granted when an organisation implements measures in order to protect personal data. At the time of the review, there were more than 5,000 participating companies.

In its report, the Commission confirms that the EU-US Privacy Shield continues to provide an adequate level of protection for transfers of personal data. It indicates that important improvements have been made to the framework, but also identifies some areas of concern. The European Data Protection Board (***EDPB***), which is invited to participate in the annual review process, published its own report on the Third Annual Joint Review on 12 November 2019, essentially confirming the findings of the Commission and making further recommendations on access by public authorities to data transferred to the US under the Privacy Shield. The annual review procedure is an important element in the construction of the Privacy Shield since its predecessor, the EU-US Safe Harbour scheme, was annulled by the Court of Justice of the European Union (***CJEU***) on 6 October 2015 (Case C-362/14). Whether the improvements actually suffice for the Privacy Shield to meet the EU requirements will be determined by the European Courts in the coming months.

In their respective reports, the EDPB and the Commission welcome the fact that the US Department of Commerce (***DoC***) and the US Federal Trade Commission (***FTC***) undertook new *ex officio* oversight and enforcement actions regarding compliance with the Privacy Shield by certified organisations. "Random spot checks" by the DoC have increased to 30 organisations per month.

However, the reports signal a lack of oversight on substantive compliance. The actions by the DoC and FTC focus on formal and procedural aspects rather than substantive aspects. In particular, the EDPB and the Commission regret the absence of checks on onward transfers of personal data to jurisdictions outside the US or EU. The European institutions consider that the DoC should use its power to demand insight into the contracts that organisations make with partners in third countries.

Other areas of focus are the application of the Privacy Shield requirements regarding human resources data, on which EU and US interpretations differ, and the re-certification process, which requires further refinement. The EDPB furthermore indicates that some of the concerns which it raised in earlier reports have not been addressed. Examples include the limitations to the rights of data subjects, the lack of specific rules on automated decision-making, and the overly broad exemption for publicly available information.

The EDPB report also voices concerns about the collection of and access to data by US public authorities for purposes of national security and law enforcement. US surveillance programmes need increased safeguards, for example, when determining whether an individual or group can be a target of surveillance. The EDPB also laments the fact that the Privacy and Civil Liberties Oversight Board (***PCLOB***) is not providing it with updated reports on specific US surveillance mechanisms and privacy safeguards, making meaningful reviews difficult.

Conversely, the EDPB and the Commission welcome the fact that, for the first time since their creation in 2016, all slots of the PCLOB have been filled. They also welcome the appointment of Keith Krach as the permanent Ombudsperson on 18 January 2019, following a European demand to that effect made in the Second Annual Review of December 2018. However, according to the EDPB, the exact powers of the Ombudsperson still have to be clarified through the disclosure of internal procedures concerning interactions between the Ombudsperson and the intelligence community. So far, the EDPB is not convinced that the Ombudsperson's powers to access information and remedy non-compliance are sufficient in the light of Article 47 of the EU Charter of Fundamental Rights, which requires an effective remedy before a tribunal.

Questions on the criteria for international transfers of personal data are currently pending before the General Court of the European Union (***GC***) and the CJEU. In Case T-738/16, French digital rights groups are claiming that the EU-US Privacy Shield fails to respect specific fundamental EU rights. A related question is before the CJEU in Case C-311/18 (more commonly known as the *Schrems II* case), in which the CJEU was requested to provide a preliminary

ruling on the validity of standard contractual clauses, and ultimately may set out general criteria for the level of protection that is required for international transfers of personal data. These criteria, in turn, could be relied on for the assessment of the EU-US Privacy Shield. In this regard, the current reports point to improvements but also areas of concern. As a result, the outcome of the cases before the EU Courts remains uncertain.

If the EU-US Privacy Shield were to be annulled, the transfers of personal data to the more than 5,000 US recipients that currently rely on the scheme would become illegal and transferring parties in the EU would have to find an alternative solution to ensure compliance with the General Data Protection Regulation (GDPR). The decisions of the CJEU and GC are expected in early 2020.

A copy of the European Commission's report can be found here. The EDPB's report can be found here.

European Data Protection Board Publishes Final Guidelines on Territorial Scope of General Data Protection Regulation

On 12 November 2019, the European Data Protection Board (***EDPB***) published the final version of its Guidelines (the ***Guidelines***) on the territorial scope of the General Data Protection Regulation (***GDPR***). The draft guidelines had been published for public consultation at the end of 2018 (See, this Newsletter, Volume 2018, No. 12, at p. 8).

With the adoption of the GDPR, the expansion of the territorial scope of EU data protection rules was considered necessary in order to provide a high level of data protection to EU data subjects, and to ensure that EU businesses compete with businesses from third countries on a level playing field. There are two criteria determining the territorial application of the GDPR which are set out in Article 3 of the GDPR: (i) the "establishment" criterion; and (ii) the "targeting" criterion. The Guidelines clarify these concepts and offer examples for each of them.

Establishment Criterion

According to the EDPB, two conditions must be satisfied in order for the GDPR to apply under the establishment criterion. First, the controller or processor needs to have *an establishment* in the EU. Second, the processing of personal data must happen i*n the context of the activities* of that establishment.

Regarding the first condition, the notion of establishment extends to any real and effective activity in a Member State exercised through stable arrangements. For an entity having its main establishment outside the EU, this can consist of a branch or a subsidiary, but it can also be a minimal activity, such as the presence of a single employee or agent in the EU, as long as that person acts with a sufficient degree of stability. By contrast, the Guidelines explain that the mere accessibility of a website in the EU is insufficient to conclude that there is an EU establishment. An EU-based processor cannot be regarded as an establishment of a non-EU-based controller.

The second condition is that the processing of personal data happens "in the context of the activities of an EU establishment". However, it is not necessary that the processing *itself* is carried out by the EU establishment. The analysis happens on a case-by-case basis. For non-EU based entities, the EDPB requires that the data processing is "inextricably linked" to the activities of the local EU establishment. An indication of such an inextricable link may be that the local EU establishment raises revenue in the EU in support of the data processing.

The place where the actual processing is carried out is irrelevant. Furthermore, the location of the data subjects is also irrelevant. For example, if an EU-based company only processes personal data of non-EU-based persons, that processing will still be subject to the GDPR.

This criterion should be applied separately to controllers and processors. It is possible that a controller is subject to the GDPR while the processor is not. In that case, only the controller is subject to all the obligations of the GDPR, but the controller may also have to impose some GDPR obligations on the processor by contract. If only the processor is subject to the GDPR, the processor will be subject to those GDPR obligations that specifically target processors.

Targeting Criterion

If an entity is not established in the EU, it may still be subject to the GDPR under the "targeting criterion". For this to apply, two conditions must be satisfied: (i) processing of personal data of data subjects in the EU; and (ii) the pro-

cessing is carried out for a specific purpose (*i.e.*, the offering of goods or services or the monitoring of behaviour).

Regarding the first condition, the legal status of the data subject in the EU is irrelevant. All natural persons in the EU are taken into account, irrespective of nationality or residence. Whether the data subject is in the EU must be assessed at the time when the targeting takes place (*i.e.,* when the goods or services are offered or when behaviour is monitored).

The data processing must be done for the purpose of offering goods or services, or for the monitoring of behaviour. As regards the first, it is irrelevant whether a payment is made or not. The offering of services also includes the offering of information society services.

It is necessary that the offering of goods or services targets data subjects in the EU. The EDPB finds inspiration in the case law of the Court of Justice of the European Union (***CJEU***) on the Brussels I Bis Regulation (which regulates the jurisdiction of the courts and the enforcement of judgments in the EU). It provides a non-exhaustive list of factors which may be taken into account to determine whether EU data subjects are targeted, including:

- whether the EU or a Member State is mentioned by name;
- whether advertisements are aimed at EU countries;
- whether the activity is of an international nature (for instance, tourism);
- whether travel instructions from an EU Member State are provided;
- whether an EU language or currency is used (which is not used in the trader's country);
- whether goods are delivered in the EU;
- whether an EU top-level domain name is used (different from the trader's country).

The second relevant activity is the monitoring of data subjects' behaviour. This includes tracking a person on the internet, but also the monitoring of behaviour through other technologies, for instance, through wearables and other smart devices.

Not *all* monitoring of behaviour is sufficient. This condition will only be triggered if the controller has a specific purpose in mind for the collection and subsequent reuse of that data. In particular, behavioural analysis and profiling techniques will be relevant. The EDPB gives a non-exhaustive list of activities that could be caught by this provision:

- behavioural advertising;
- geo-localisation services;
- online tracking through cookies or other techniques;
- health analytics;
- closed circuit television.

Finally, under the targeting criterion, the EDPB explains that the status of the processor follows the status of the controller. When a controller satisfies this criterion, the processor will automatically meet it too.

Entities subject to the GDPR under the targeting criterion have an obligation to appoint a representative in an EU Member State where their targeting takes place. The EDPB therefore ends its Guidelines with a section on the EU representative: how to appoint one, when exemptions apply, and what the obligations and responsibilities of the representative are. The main duty of the representative is to facilitate communication between the controller or processor, EU data subjects and supervisory authorities.

The Guidelines can be consulted here.

INTELLECTUAL PROPERTY

Can Work of Art Contain Well-known Trade Mark?

On 14 October 2019, the Benelux Court of Justice (the ***BCJ***) ruled on the question whether a work of art can contain a well-known trade mark.

In the case at hand, Cedric Peers, a Belgian artist, painted champagne bottles with the recognisable shape and accentuated label of Dom Pérignon Champagne (see picture below). The artist made several paintings along the same theme in which the Dom Pérignon trade marks are clearly identifiable or which amount to playful variations on these trade marks. The paintings were sold by the painter as the '*Damn Pérignon*' series. The works have an ironic and sometimes also erotic character. In addition to the paintings, Cedric Peers also offers for sale textile products which, according to Moët Hennessy Champagne Services, bear signs which are very similar to those of Dom Pérignon trade marks.

The design of the characteristic bottles with a long neck and a shield shaped label with the name 'Dom Pérignon' was created for Moët Hennessy Champagne Services by Andy Warhol. Moët Hennessy Champagne Services, which had also registered these items as Pérignon trade marks, brought an action against Mr. Peers before the Dutch-language Enterprise Court of Brussels (*Ondernemingsrechtbank/tribunal de l'entreprise*) for infringement of its trade marks.

The Enterprise Court of Brussels referred a question to the BCJ as regards Article 2.20(2)(d) of the Benelux Convention on Intellectual Property to learn: (i) whether the freedom of expression and, in particular, artistic freedom as protected by Article 10 of the European Convention on Human Rights and Article 11 of the Charter of Fundamental Rights of the European Union can constitute "due cause" for using a trade mark; and (ii) if yes, under what conditions.

In its judgment, the BCJ refers to a judgment of the Court of Justice of the European Union (the ***CJEU***) of 6 February 2014 in the case *Leidseplein Beheer* (Case C-65/12) in which the CJEU held that, "[i]*t follows that the concept of 'due cause' may not include objectively overriding reasons but may also relate to the subjective interests of a third party using a sign which is identical or similar to the mark with a reputation*". The concept of "due cause" is intended to strike a balance between the rights of the trade mark holder and the interests of a third party user of the sign. The BCJ also takes account of recital 27 of Directive 2015/2436 on trade marks according to which "[u]*se of a trade mark by third parties for the purpose of artistic expression should be considered as being fair as long as it is at the same time in accordance with honest practices in industrial and commercial matters. Furthermore, this Directive should be applied in a way that ensures full respect for fundamental rights and freedoms, and in particular the freedom of expression*".

Therefore, according to the BCJ, artistic freedom as part of the protected right of freedom of expression of the artist, can be a valid reason for the use of a trade mark or a similar sign other than for distinguishing goods or services, if there is an artistic expression that is the original result of a creative design process and which does not aim to harm the trade mark or the trade mark holder. It will now be for the Enterprise Court of Brussels to make this assessment in the light of the particular circumstances of the case.

Access to Company Systems by Former Employee Does Not Necessarily Infringe Business Secrets

On 16 October 2019, the Enterprise Court of Antwerp (the ***Court***) handed down a judgment in which it held that not every, even sensitive, business information can be regarded as a "*business secret*" protected by Article I.17/1 of the Code of Economic Law (Wetboek van Economisch Recht / Code de droit économique; the ***Code of Economic Law***).

The case follows the dismissal of an employee by his employer (called Jas) in February 2019. Following the dismissal, the parties entered into a settlement agreement according to which the employee's last working day would be 8 March 2019. In late March 2019, the employee concluded a new employment agreement with Crane, a competitor of Jas.

During his time with Jas, the employee had access to an online Customer Relationship Management system called "Zoho" (***Zoho***). Zoho contained business information about Jas (*i.e.*, mainly information about its invoicing and client orders).

On 1 March 2019, during a job interview with Crane, the employee logged in with his old user credentials in to the Zoho system to show the usefulness of the web application to his new employer. Jas noticed that the former employee had logged in to its systems and thus sued the former employee for infringing "*business secrets*" within the meaning of Article I.17/1 of the Code of Economic Law.

In its judgment, the Court held that business information can only be regarded as a "*business secret*" under Article I.17/1 of the Code of Economic Law if it is not easily accessible for persons who have experience in dealing with that kind of information. The Court went on to say that in the case at hand it was easy for Crane to gain access to the business information contained in the Zoho system by its own knowledge of the market since it was a competitor of Jas. The Court added that Jas had failed to demonstrate that the business information included in Zoho had a commercial value.

The Court concluded that the business information disclosed to Crane by the employee did not constitute a "*business secret*" protected under the Code of Economic Law and, therefore, rejected the action brought by Jas.

Court of Justice of European Union Clarifies Competence of National Courts for Interim Enforcement of Community Designs

On 21 November 2019, the Court of Justice of the European Union (the ***CJEU***) delivered a judgment pursuant to a request for a preliminary ruling by the Supreme Court of the Netherlands (*Hoge Raad der Nederlanden*) on the interpretation of Article 90(1) of Regulation 6/2002 of 21 December 2001 on Community designs.

Regulation 6/2002 requires Member States to designate national courts competent to hear cases about Community designs. Its Article 90(1) provides that an application for protective measures of a Community design may be filed before the national courts, including Community design courts, even if a Community design court of another Member State has jurisdiction on the substance of the matter.

The main proceedings in the framework of which the preliminary ruling was requested concerned the marketing of a toy product by High5 Products. That company received a notice from Spin Master demanding that the product be removed from the market. Spin Master claimed it had registered the product design before High5 Products started marketing its product.

As High5 Products failed to heed the notice, Spin Master applied for interim relief before the District Court of Amsterdam (*Rechtbank Amsterdam*). The District Court of Amsterdam held that it had jurisdiction to decide on Spin Master's request. However, the Prosecutor General at the Supreme Court of the Netherlands (*Procureur-Generaal bij de Hoge Raad der Nederlanden*) contested the competence of the court and appealed to the Supreme Court of the Netherlands (*Hoge Raad der Nederlanden*). The Prosecutor General argued that according to Regulation 6/2002, the District Court of The Hague (*Rechtbank Den Haag*) had exclusive jurisdiction in Community design matters, including protective measures, such as those requested by Spin Master.

The Supreme Court of the Netherlands stayed the proceedings and referred a question to the CJEU for a preliminary ruling. It sought to know whether the exclusive jurisdiction conferred by Regulation 6/2002 on Community design courts is extended to the substance of a dispute and provisional measures or, rather, if other courts in the Member State – with jurisdiction to decide on protective

measures related to a national designs – have jurisdiction to decide on protective measures related to Community designs.

The CJEU considered that, pursuant to the wording of Article 90(1) of Regulation 6/2002, a design right holder may apply for protective measures, not only to the Community design courts of a Member State, but also to any court or tribunal in such Member State with jurisdiction to adopt such protective measures in respect of national designs. The CJEU held that although the objective of Regulation 6/2002 – in assigning exclusive jurisdiction on Community designs to specific courts – is to develop a uniform interpretation of the requirements governing the validity of those designs, such an objective is justified only in the case of court proceedings on the substance of infringement or invalidity actions regarding Community designs.

The CJEU recalled that Regulation 6/2002 provides that a Community design must be enforced in an efficient manner throughout the territory of the European Union. It added that, in the case of requests for protective measures, the requirements of proximity and efficiency should prevail over the objective of specialisation.

In view of the above, the CJEU confirmed that Article 90(1) of Regulation No 6/2002 allows the courts and tribunals of the Member States with jurisdiction to order provisional measures, including protective measures, with regard to national designs also to have jurisdiction to deal with such measures in respect of a Community design.

LABOUR LAW

Demoting Female Employee on Return From Maternity Leave Followed By Parental Leave Constitutes Form of Discrimination

Background of Case

An employee entered into service in 2009 (the ***employee***). As of mid-July 2016, the employee was on maternity leave followed by a parental leave of three months.

On her return from parental leave in February 2017, the employee was informed of a company reorganisation that affected her department. She quickly realised that she was being demoted as a result of the reorganisation. A few weeks after her return, the employee resigned and brought the matter before the Brussels Dutch-language Labour Court (the ***Labour Court***). She claimed that the employer did not allow her to return to an equivalent job after the end of her parental leave. She argued that the employer had thus violated the Law of 10 May 2017 which prohibits gender-based discrimination in various areas, including labour relations (the ***Gender Law***).

Judgment of Labour Court

On 3 September 2019, the Labour Court handed down its judgment.

First, the Labour Court referred to the case law of the Constitutional Court which holds that when an employee invokes facts that may give rise to a presumption of discrimination, it is for the employer to prove that there was no such discrimination.

Second, the Labour Court observed that the Gender Law does not contain any provision implementing Article 15 of Directive 2006/54 of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation. This provision expressly provides that a woman returning from maternity leave is entitled to take up the exact same position which she held before her absence or an equivalent position.

According to the Labour Court, this entitlement stems from the prohibition to modify an employment agreement unilaterally (Article 1134 of the Civil Code and Article 20, §1, 1° of the Law of 3 July 1978 on employment contracts) and the prohibition to discriminate on the basis of gender, as set forth in the Gender Law.

On this basis, the Labour Court reached the conclusion that a failure to comply with the obligation to provide an employee with the same or equivalent position upon her return from maternity and/or parental leave must be regarded as unfavourable treatment. The employer must in such an event prove that the change of position is not related to the maternity and/or parental leave but is justified by other reasons.

In the case at hand, the Labour Court established that the employee had been demoted on her return from parental leave which resulted in a presumption of discrimination. The Labour Court also noted that the employer was unable to provide sufficient evidence that this demotion was not related to her maternity and/or parental leave. Hence, the employer was not able to demonstrate the alleged company restructuring.

The Labour Court therefore concluded that the employee had been discriminated against on the grounds of gender and awarded the employee an indemnity of six months' gross remuneration.

Practical Implications

This judgment shows that an employer is obliged to ensure that an employee returning from maternity and/or parental leave is permitted to take up the same or an equivalent position as she had before her absence. If not, the employer may be held liable to pay six months' gross remuneration on top of the severance pay, unless he is able to prove that a possible demotion was not related to the maternity and/or parental leave. This constitutes a high burden of proof.

LITIGATION

Cross-Border Debt Recovery: Court of Justice of European Union Rules on European Account Preservation Order Procedure

On 7 November 2019, the Court of Justice of the European Union (the ***CJEU***) handed down a judgment in which it held that if a creditor wishes to rely on an order for payment in order to benefit from the European Account Preservation Order (***EAPO***) procedure against a debtor, this order for payment must be enforceable under the relevant domestic law.

Regulation 655/2014

Regulation 655/2014 of 15 May 2014 establishing an EAPO procedure to facilitate cross-border debt recovery in civil and commercial matters (***Regulation 655/2014***) entered into force on 18 January 2017 (See, this Newsletter, Volume 2017, No. 1, p. 6).

Regulation 655/2014 allows a creditor, domiciled in one Member State, to request the courts of a Member State to issue an EAPO in order to preserve the funds held by a debtor in a bank account located in another Member State. The EAPO thus prevents a debtor from jeopardising the creditor's claim by transferring or withdrawing those funds.

The application for an EAPO should be made by a creditor through a standard multilingual form filed before, during or after the legal proceedings on the substance of the claim have taken place. The creditor must file his application before the courts of the Member State which either had jurisdiction to rule on the "*substance of the matter*" or which gave the judgment, the court settlement or the "*authentic instrument*" that serves as the basis for the EAPO.

Facts

In its judgment of 7 November 2019, the CJEU clarified the scope and content of the notions of "*authentic instrument*" and "*substance of the matter*" under Regulation 655/2014.

In the case at hand, a creditor had obtained a payment order (the ***Payment Order***) from a Bulgarian District Court (the ***District Court***) to recover specific debts against various debtors. The creditor then requested an EAPO from the same District Court in order to attach the funds held on the debtors' bank accounts in Sweden.

However, the District Court considered that the Payment Order did not constitute a valid "*authentic instrument*" pursuant to Regulation 655/2014, since it was unenforceable under Bulgarian law. The District Court therefore referred the matter back to the President of the District Court of Sofia (the ***President***) who, according to the District Court, had jurisdiction to rule on the "*substance of the matter*".

The President, however, disagreed and referred the matter back to the District Court, arguing that the Payment Order, albeit unenforceable, constituted an "*authentic instrument*" under Regulation 655/2014 and that the District Court was thus competent to issue the EAPO.

In order to settle this jurisdictional dispute, the District Court referred a request for a preliminary ruling to the CJEU for interpretation of Regulation 655/2014.

CJEU's Judgment

In its judgment, the CJEU held that a payment order can only be considered as an "*authentic instrument*" if it is enforceable under the relevant domestic law. In the case at hand, since the Payment Order was unenforceable under Bulgarian law, it did not constitute a valid "*authentic instrument*" and, therefore, the EAPO could only be sought before the Bulgarian court that had jurisdiction to rule on the "*substance of the matter*".

The CJEU also held that the procedure to request a Payment Order before the District Court had to be considered as a procedure on the "*substance of the matter*" since the latter was defined by Recital 13 of Regulation 655/2014 as being "*any proceedings aimed at obtaining an enforceable title on the underlying claim including, for instance, summary*

proceedings concerning orders to pay and proceedings such as the French 'procédure de référé'".

The CJEU therefore concluded that the District Court had jurisdiction to issue the EAPO.

EU Council Revises and Approves Proposed Directive on Collective Representative Actions

On 28 November 2019, the Council of the European Union (the ***Council***) revised and approved the proposed Directive on representative actions for the protection of the collective interests of consumers (the ***Draft Directive***).

The Draft Directive was initially proposed by the European Commission in April 2018 (See, this Newsletter, Volume 2018, No. 4, p. 19) and was then examined, in first reading, by the European Parliament (the ***EP***).

The Draft Directive aims to empower qualified entities, such as consumer organisations, to seek, in addition to injunctions, redress measures, including compensation or replacement, on behalf of a group of consumers that has been harmed by a trader in areas such as data protection, financial services, travel and tourism, energy and telecommunications.

In its assessment, the Council amended the Draft Directive in order to distinguish between qualified entities entitled to bring domestic representative actions and those entitled to bring cross-border representative actions. The former will have to satisfy the criteria set out in the law of the Member State of designation, whereas the latter will have to satisfy the harmonised criteria spelled out in the Draft Directive itself. Those criteria include:

- Being a legal person properly constituted according to the law of the Member State of designation 18 months prior to the designation request and demonstrating 12 months of actual public activity in the protection of consumers' interests;
- Having a legitimate interest in protecting consumer interests;
- Having a non-profit making character;
- Being in a sound and stable financial situation;
- Not being influenced by persons, other than consumers, who have an economic interest in the bringing of any representative action.

According to the amendments made by the Council, the Draft Directive will also require EU Member States to choose expressly between an opt-in and an opt-out system. In an opt-in system, consumers will be required to express their wish to be represented by the qualified entity for the purpose of a particular representative action. In an opt-out system, consumers who do not wish to be represented by the qualified entity for the purpose of a particular representative action will be required to make a statement to that effect.

The revised version of the Draft Directive will now be discussed in second reading in the European Parliament.

PUBLIC PROCUREMENT

New EU Public Procurement Thresholds

On 31 October 2019, the Official Journal of the EU published new financial thresholds for the application of the EU public procurement Directives.

The new thresholds, which will apply from 1 January 2020, are as follows (VAT excluded):

- Directive 2014/24/EU of 26 February 2014 on public procurement ("classical sectors"):

Type of contract	Current threshold (EUR)	New threshold (EUR)
Supplies and services - Central government authorities	144,000	139,000
Supplies and services - Sub-central contracting authorities	221,000	214,000
Works	5,548,000	5,350,000
Light touch regime (social and other services listed in Annex XIV)	750,000	750,000

- Directive 2014/25/EU of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors:

Type of contract	Current threshold (EUR)	New threshold (EUR)
Supplies and services	443,000	428,000
Works	5,548,000	5,350,000
Light touch regime (social and other services listed in Annex XIV)	1,000,000	1,000,000

- Directive 2009/81/EC of 13 July 2009 on the coordination of procedures for the award of specific works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security:

Type of contract	Current threshold (EUR)	New threshold (EUR)
Supplies and services	443,000	428,000
Works	5,548,000	5,350,000

- Directive 2014/23/EU of 26 February 2014 on the award of concession contracts:

Type of contract	Current threshold (EUR)	New threshold (EUR)
Concession contracts	5,548,000	5,350,000

Contracts whose estimated value equals or exceeds the above thresholds must be announced both in the Belgian Public Tender Bulletin (*Bulletin der Aanbestedingen / Bulletin des Adjudications*; available here), and in the Supplement to the Official Journal of the EU (available here). The slight decrease in thresholds implies that, as from 1 January 2020, more public procurement procedures will be subject to the EU public procurement rules.

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