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

Legal 500 2019

October 2020

VBB on Belgian Business Law

Highlights

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

IFLR1000, 2019

Topics covered in this issue

vbb@vbb.com
www.vbb.com

Table of contents

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

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

COMPETITION LAW

European Commission Opens In-depth State Aid Investigation into Belgian Capacity Mechanism

On 16 October 2020, the European Commission (the ***Commission***) published a notice (the ***Notice***) inviting interested third parties to comment on Belgium's proposed Capacity Mechanism (the ***CM***).

The Notice was published as part of an in-depth State aid investigation launched by the Commission on 21 September 2020 (*See, this Newsletter, Volume 2020, No. 9, p. 3*). The CM aims to ensure the security of supply of electricity and resource adequacy following the scheduled closure of the last nuclear power plant in 2025.

However, the Commission has doubts regarding the CM's necessity, appropriateness and proportionality and is concerned about its impact on competition and trade.

First, the Commission wonders whether Belgium properly quantified its adequacy requirements. The support provided for by the CM may exceed what is necessary to satisfy adequacy needs and may result in over-procurement of capacity. In addition, the Commission has doubts regarding the proportionality of the volume of electricity to be procured and the quantities needed for the security of supply.

Second, the Commission's preliminary view is that the CM may, in its current form, prevent fair competition between technologies equally contributing to resource adequacy. Intermittent technologies with high de-rating factors (such as solar and wind renewable energy sources) may be deterred from participating in the CM. (The purpose of de-rating factors is to evaluate the contribution of different technologies (generation; demand flexibility; and storage facilities) to the adequacy for a particular input scenario).

Third, the Commission is concerned that the CM may discriminate against cross-border capacity. While cross-border capacity can participate in the CM from the first auction onwards, indirect foreign capacity will only be eligible for one-year contracts and may be subject to an intermediate price cap. The Commission takes the preliminary view that the conjunction of these two factors will prevent these capacities from submitting their true costs in the auction in case they are higher than the intermediate price cap, which may dissuade them from participating in the CM.

Finally, the Commission considers it necessary to verify whether the CM incentivises additional interconnection between Belgium and its neighbouring countries.

European Commission Opens In-depth State Aid Investigation into Authorisation Granted by Belgium to Ladbrokes to Operate Virtual Betting

On 23 October 2020, the European Commission (the ***Commission***) published a notice (the ***Notice***) inviting interested third parties to comment on the authorisation granted by Belgium to Derby NV, a local subsidiary of the betting and gambling company Ladbrokes PLC and operating in Belgium under the commercial name "Ladbrokes" (***Ladbrokes***), to operate virtual betting (the ***Authorisation***).

The Notice forms part of the in-depth State aid investigation started by the Commission on 2 September 2020 further to a complaint by Rocoluc NV and European Amusement Company NV. According to the plaintiffs, the Authorisation conferred on Ladbrokes the *de facto* exclusive right to operate virtual betting in Belgium without appropriate remuneration. The plaintiffs consider that this amounts to illegal State aid.

The Notice mentions that the Gaming Commission (*Kanspelcommissie / Commission des jeux de hasard*), Belgium's federal authority in charge of granting licences to gaming establishments, issued the Authorisation through e-mails of 10 February 2014 and 5 March 2015. The Gaming Commission subsequently denied other establishments the authorisation to operate virtual betting, explaining its refusal by referring to the ongoing assessment of the classification of virtual betting. However, the Gaming Commission did not suspend the regulatory framework or Ladbrokes' Authorisation until 1 July 2017. In addition,

Ladbrokes continued to offer virtual betting services in its betting outlets even after the suspension decided by the Gaming Commission in 2017, leading several gaming operators to take legal action against Ladbrokes.

Interested parties are invited to submit their comments to the Commission by 23 November 2020.

Brussels Court of Appeal Partially Annuls 2009 Decision Imposing Record Fine on Proximus for Margin Squeeze Abuse But Provisionally Maintains Fine

On 7 October 2020, the Markets Court of the Brussels Court of Appeal (*Marktenhof / Cour des marchés*) (the ***Markets Court***) partially annulled the decision of 26 May 2009 (the ***2009 Decision***), for lack of admissible evidence, by which the Belgian Competition Authority (*Belgische Mededingingsautoriteit / Autorité belge de la Concurrence*) (***ABC***), formerly called Belgian Competition Council, had found Proximus (formerly Belgacom) guilty of margin squeeze in 2004 and in 2005, in breach of Article IV.2 of the Code of Economic Law (*Wetboek van Economisch Recht / Code de droit économique*) and its equivalent under EU law, Article 102 of the Treaty on the Functioning of the European Union.

This judgment is the consequence of another judgment of 9 October 2019 in which the Market Court had found the dawn raids carried out at the premises of Proximus on 19 January 2006 to be illegal because they were not authorised by a judge, and were in breach of Proximus' right to privacy. As a result, all documents seized during that dawn raid had to be removed from the investigation file. Proximus then argued that the remaining evidence was insufficient to support the 2009 Decision and that this decision – including the record fine of € 66.3 million which the BCA imposed on Proximus – should be annulled.

The Markets Court analysed this argument by following a two-step reasoning.

As a first step, the Markets Court looked at the origin of the data used by the BCA in its 2009 Decision and identified three possibilities.

- First possibility: the data does not originate directly or indirectly from the dawn raid. In this case, the data can be maintained in the investigation file.
- Second possibility: the data comes directly from the dawn raid. It cannot be used and must be set aside.
- Third possibility: the data comes indirectly from the dawn raid. In this third scenario, it is necessary to proceed to the second step of the reasoning.

The second step of the reasoning followed by the Markets Court is to determine whether the dawn raid was "indispensable" to access the data which indirectly comes from it. If the dawn raid was not indispensable, meaning that this data could have been collected by other means, then the data can be kept in the investigation file. If, conversely, the dawn raid was indispensable to the collection of the data, *i.e.*, this data could not have been obtained by other means, then the data must be permanently removed from the investigation file and cannot serve as a basis for a statement of objections or for a final decision such as the 2009 Decision.

The Court also made clear that the validity of the infringement decision adopted by the BCA in 2009 must be determined by verifying if, after removing all evidence emanating from the 2006 dawn raid (using the above methodology), the remaining evidence referred to in the decision is sufficient to support it. In other words, the BCA cannot justify the validity of its decision by referring to evidence that is in the investigation file but not in the 2009 Decision.

Based on this methodology, the Markets Court considered that the 2009 Decision could not be upheld concerning the part of the infringement that took place in 2004. By contrast, the Markets Court found that there was sufficient evidence remaining in the 2009 Decision to support the findings of the BCA regarding the year 2005.

Interestingly, the Markets Court did not annul the fine imposed on Proximus. The Markets Court indicated that there was evidence of an infringement taking place in 2005. In addition, contrary to Proximus' assertion, the fine for this infringement does not amount to half of the total fine imposed by the BCA for the years 2004 and 2005, as the calculation of a competition law fine is based on several factors that can vary from one year to the next and for which the BCA enjoys a margin of appreciation. Finally, the Markets Court observed that the appeal procedure is not yet complete. It is therefore necessary to wait for the Markets Court to rule on the remaining pleas put forward

by Proximus before sending the case back to the BCA in order to reassess the amount of the fine, should that prove necessary.

Brussels Court of Appeal Annuls Belgian Competition Authority's Decision Rejecting Football Club Virton's Request for Interim Measures

In a judgment delivered on 23 September 2020, the Markets Court of the Brussels Court of Appeal (*Marktenhof / Cour des marchés*) (the ***Markets Court***) annulled the decision adopted on 29 June 2020 by the Competition College (*Mededingingscollege / Collège de la concurrence*) of the Belgian Competition Authority (*Belgische Mededingingsautoriteit / Autorité belge de la Concurrence* - the ***BCA***) refusing to grant the interim measures requested by Belgian football club Royal Excelsior Virton (***Virton***) against the Royal Belgian Football Association (the ***RBFA***) (*See, this Newsletter, Volume 2020, No. 6, p. 6, and Volume 2020, No. 7, p. 3*).

RBFA had refused to issue a new operating licence to Virton because that club did not comply with the continuity principle. Virton was instead relegated to a lower tier in the competition. Virton complained to the BCA that RBFA had restricted competition and requested interim measures. The Competition College of the BCA rejected this request. The BCA found that, although subjecting the participation in the championship to the condition of obtaining a licence and requiring that the clubs concerned comply with the continuity principle may restrict competition, these conditions seem *prima facie* to pursue the legitimate objective of allowing an orderly competition. The BCA also considered that the application of the continuity principle was proportionate and legitimate to the objective pursued. While "it cannot be *prima facie* excluded" that some criteria applied by the RBFA are problematic, the BCA found that Virton did not establish that it would have satisfied the conditions to obtain a licence absent these problematic criteria.

The Markets Court found that the BCA could not consider that "it cannot be prima facie excluded" that some criteria used by RBFA are disproportionate in relation to the objective pursued, while maintaining that it is not *prima facie* established that Virton would have satisfied the criteria to obtain a licence absent these problematic criteria. These assertions were made in circumstances in which Virton had proven that it does not have social security debts or debts vis-à-vis third parties. In addition, the BCA acknowledged that the assessment of a request for a licence infringes competition law if it is carried out based on excessively rigid criteria. According to the Markets Court, it was therefore necessary for the BCA to rule on this issue and determine if the criteria were effectively disproportionate and therefore prima facie illegal. The Markets Court held that the BCA could have explained in its decision that the RBFA's conditions were disproportionate but that these conditions were nevertheless satisfied, and that, prima facie, Virton would therefore have satisfied the conditions for a licence absent the problematic conditions.

In addition, the BCA held that a sponsoring requirement included in point 17 of the RBFA's document "could be disproportionate with the legitimate objective of ensuring and controlling the continuity of the football clubs" while at the same time concluding that there was no prima facie infringement of the competition rules. The Markets Court found these positions to be contradictory.

Finally, the Markets Court held that the BCA could have established that Virton satisfied the continuity principle (applied in accordance with competition law) if it had not failed to take the relevant evidence into consideration.

As a result, the Markets Court concluded hat the BCA had not adequately provided reasons for its decision to refuse to grant interim measures to Virton. The Markets Court therefore annulled the BCA decision and referred the case back to the BCA.

CONSUMER LAW

Federal Chamber of Representatives Adopts Law on Cooperation Between National Authorities Responsible for Enforcement of Consumer Protection Laws

On 24 September 2020, the federal Chamber of Representatives adopted a Bill modifying the Code of Economic Law (the ***CEL***) in order to implement Regulation (EU) 2017/2394 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Consumer Protection Cooperation Regulation or ***CPC Regulation***) (*Wetsontwerp tot wijziging van het Wetboek van Economisch Recht en van andere wetten met het oog op het versterken van de opsporings- en handhavingsbevoegdheden in overeenstemming met en in uitvoering van Verordening (EU) 2017/2394 van het Europees Parlement en de Raad van 12 december 2017 betreffende samenwerking tussen de nationale autoriteiten die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming / Projet de loi modifiant le Code de droit économique et d'autres lois en vue de renforcer les compétences de recherche et d'application conformément au règlement (UE) 2017/2394 du Parlement européen et du Conseil du 12 décembre 2017 sur la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs* – the ***Bill***).

The CPC Regulation establishes a cooperation framework to enable national enforcement authorities to deal jointly with infringements of consumer protection laws when traders and consumers are established in different EU Member States. The CPC Regulation ensures that national authorities have sufficient enforcement powers and provides for common procedures for coordinated actions as well as an enhanced mechanism for the exchange of information between national authorities. The Chamber of Representatives decided to modify the CEL to ensure the adequate application in Belgium of the CPC Regulation following its entry into force on 17 January 2020.

First, the Bill broadens and clarifies the investigative powers of national authorities when enforcing consumer protection laws. Enforcement authorities are now entitled to investigate and monitor financial flows. To this end, they may request information on financial transactions from financial institutions. They are also allowed to make test purchases using a fictitious identity and to approach companies whilst pretending to be customers.

Second, the Bill enables the enforcement authorities to adopt interim measures when these are necessary to avoid harm to consumers. In that respect, and subject to strict conditions, the authorities can (i) remove content from, or restrict access to, an online interface; (ii) make websites inaccessible; and (iii) order domain name registrars to delete a specific domain name.

Third, the Bill confers on the enforcement authorities the power to accept commitments from companies to bring their infringements to an end and, if appropriate, to adopt corrective measures. The authorities are allowed to publish such commitments. Furthermore, the Bill modifies the provisions on penalties and introduces the possibility to impose administrative fines for infringements of consumer protection laws.

Fourth, enforcement authorities are entitled to publish temporarily lists of companies that fail to comply with consumer protection laws, after having informed the companies concerned. This publication must be withdrawn as soon as the companies provide evidence that they have brought the infringement to an end.

Finally, the Bill provides that the new tools that apply to cross-border consumer law infringements also apply to infringements committed by Belgian companies against Belgian consumers. This is to ensure that Belgian consumers are granted the same protection as other EU consumers.

The Bill adopted by the Chamber of Representatives will enter into force ten days after its publication in the Belgian Official Journal (*Belgisch Staatsblad / Moniteur belge*).

Court of Justice of European Union Rules on Calculation of Contract Price after Exercise of Right of Withdrawal from Distance or Off-premise Contracts

On 8 October 2020, the Court of Justice of the European Union (the ***CJEU***) delivered a judgment clarifying Article 14(3) of Directive 2011/83/EU of 25 October 2011 on consumer rights (the ***Directive***) (CJEU, 8 October 2020, Case C-641/19, *PE Digital*). Article 14(3) of the Directive reads as follows:

"*Where a consumer exercises the right of withdrawal after having made a request in accordance with Article 7(3) or Article 8(8) [i.e., a request for the performance of services to begin already during the 14-day withdrawal period applicable to distance and off-premise contracts], the consumer shall pay to the trader an amount which is in proportion to what has been provided until the time the consumer has informed the trader of the exercise of the right of withdrawal, in comparison with the full coverage of the contract. The proportionate amount to be paid by the consumer to the trader shall be calculated on the basis of the total price agreed in the contract. If the total price is excessive, the proportionate amount shall be calculated on the basis of the market value of what has been provided.*"

The judgment was given in response to a request for a preliminary ruling by a Hamburg court in a dispute between an unidentified consumer (***E.U.***) and PE Digital GmbH (***PE Digital***), a German company operating an online dating service. The dispute concerned the amount owed by E.U. to PE Digital following the exercise by E.U. of his right to withdraw from his contract with PE Digital. E.U. had subscribed to a twelve-month premium membership to PE Digital's online dating service for the price of EUR 523.95. Four days later, E.U. exercised his right of withdrawal, at which point in time E.U. was charged the amount EUR 392.96. Having initiated proceedings before the Hamburg court, E.U. claimed to be entitled to the full reimbursement of the price paid. He argued that the services had only been performed during the withdrawal period and that the contract price was excessive.

The Hamburg court decided to stay the proceedings and to refer a question to the CJEU on how to calculate the amount owed by the consumer upon the exercise of his right of withdrawal. The CJEU was requested to clarify whether (i) the amount owed should be calculated based on the price agreed for the full coverage of the contract and then reduced *pro rata temporis*; or whether (ii) taking account of the fact that one or more services covered by the contract was/were provided to the consumer in full before the exercise of his right of withdrawal, the amount owed should be calculated on the value of the services already performed.

The CJEU held that Article 14(3) of the Directive should be interpreted as meaning that when the consumer explicitly requests that the performance begins during the withdrawal period and then exercises his right of withdrawal, the amount owed by the consumer should be calculated based on the price agreed in the contract and then reduced *pro rata temporis*. It is only if the contract provides expressly that one or more of the services are to be provided in full from the beginning of the performance of the contract term and separately, for a price which must be paid separately, that the full price for such a service can be taken into account in the calculation of the amount owed by the consumer.

Finally, the CJEU held that, in order to determine whether the total contract price is excessive, the national court should consider the price of the service offered by the trader concerned to other consumers under the same conditions and the price of an equivalent service provided by other traders at the time of the conclusion of the contract.

European Commission Presents Digital Finance and Retail Payments Strategies

On 24 September 2020, the European Commission (the ***Commission***) presented a Digital Finance Package intended to encourage competitiveness and innovation in the financial sector. The Digital Finance Package aims to increase consumer choice and opportunities in financial services and modern payments, while at the same time ensuring consumer protection and financial stability. The Package rests on four pillars: (i) a Digital Finance Strategy; (ii) a Retail Payments Strategy; (iii) legislative proposals for an EU regulatory framework on crypto-assets; and (iv) proposals for an EU regulatory framework governing digital operational resilience. The first and second pillars are of particular relevance to consumers and businesses.

Digital Finance Strategy

The Digital Finance Strategy aims for financial services in the EU to become more digital-friendly, while regulating the risks inherent to the digital transformation of finance. The strategy identifies four priorities. First, it aims to tackle fragmentation in the Digital Single Market, thereby creating access for European consumers to cross-border services. This should give rise to new funding channels for SMEs (notably Fintech start-ups), which would allow them to scale up and be able to provide online services. Second, it seeks to adapt the EU regulatory framework to facilitate digital innovation. The strategy should ensure that innovations based on or making use of blockchain or artificial intelligence (AI) are used in line with EU standards. These innovations should create opportunities to develop better financial products for consumers, including for people currently unable to access financial services. Third, it intends to create a European financial data space to promote data-driven innovation. Fourth, it aims to address the challenges and risks associated with digital transformation: safeguarding financial stability, consumer protection, market integrity, fair competition and security.

The Commission intends to work closely with national legislators and the supervisory community at both EU and national levels to roll out this strategy in the next four years. The Communication from the Commission on a Digital Finance Strategy for the EU is available here.

Retail Payments Strategy

The Retail Payments Strategy focuses on achieving a fully integrated retail payments system in the EU, making instant payment and EU-wide payment solutions possible. Payment services should be safe, fast and reliable. First, the Retail Payments Strategy seeks to promote cross-border European payment solutions. More specifically, instant payments should become the new normal, while cash solutions should remain available and accepted. In this respect, the Retail Payments Strategy aims to increase consumer trust in instant payments by addressing risks such as real-time fraud, money laundering and cyber-attacks. Second, the Retail Payments Strategy intends to develop a competitive and innovative payments market, notably by ensuring that the relevant regulatory framework encompasses all important players in the payments ecosystem, including technology companies, and the wide adoption of the highest security standards. Third, it pursues the improvement of payment infrastructure by enhancing interoperability of infrastructures processing instant payments and facilitating mobile contactless payments. Finally, it intends to make international payments more efficient, thereby supporting the international role of the Euro currency.

To achieve the objectives of the Retail Payments Strategy, the Commission will take a number of important steps in the next four years and encourages all stakeholders, at both EU and national levels, to participate in its implementation. The Communication from the Commission on a Retail Payments Strategy for the EU is available here.

CORPORATE LAW

Ultimate Beneficial Owner Register: Additional Disclosure Obligations

On 23 September 2020, the Royal Decree amending the Royal Decree of 30 July 2018 regarding the functioning of the Ultimate Beneficial Owner Register was adopted (the ***UBO Register***) (*Koninklijk Besluit tot wijziging van het Koninklijk Besluit van 30 juli 2018 betreffende de werkingsmodaliteiten van het UBO-register / Arrêté royal modifiant l'arrêté royal du 30 juillet 2018 relatif aux modalités de fonctionnement du registre UBO* - the ***Decree***).

The UBO Register was introduced in Belgium as part of the implementation of the fourth anti-money laundering Directive 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (*See, this Newsletter, Volume 2017, No. 8, p. 12*). The regulatory framework of the UBO Register was further defined in a Royal Decree which specifies the information regarding the ultimate beneficial owner(s) of specific entities must be registered in the UBO Register (*See, this Newsletter, Volume 2018, No. 8, p. 7*).

In addition to various technical modifications regarding the access to, and functioning of, the UBO Register, the Decree now also introduces the obligation to submit supporting documents demonstrating that the registered information in relation to the ultimate beneficial owners is sufficient, accurate and correct.

While the Decree does not contain any specific provisions on the type of documents that must be submitted, the Federal Public Service Finance clarified in separate guidance that the specific documents to be submitted depend on the particular circumstances and may be a copy of the share register, articles of association, shareholders' agreements, notary deeds, or other documents. The submitted documents will not be publicly accessible and can only be consulted by the competent authorities.

The Decree entered into force on 11 October 2020. Entities registering their ultimate beneficial owners after this date must immediately submit the required supporting documents as well. The entities that had already registered their ultimate beneficial owners must submit these supporting documents before 30 April 2021.

Supreme Court Confirms Duty of Supervision of Each Board Member of Non-Profit Organisation

On 9 October 2020, the Supreme Court (*Hof van Cassatie / Cour de Cassation*) delivered a judgment regarding the duty of supervision that rests on each member of the board of directors of a non-profit organisation (***NPO***).

The defending director had argued before the Antwerp Court of Appeal that she could not be held liable for the late submission of tax returns as she had not taken on an active director's role. The defendant had also contended that she had never acted as a director and that her signature (she was the treasurer) and that of the chairman were always required for the tax and financial actions of the NPO. The Antwerp Court of Appeal held that, given these circumstances, the defendant could not be held personally liable for the late filing of the NPO's tax return.

Pursuant to Article 13, paragraph 2 of the Law of 27 June 1921 on non-profit organisations, foundations and European political parties and foundations (the ***NPO Law***) (now replaced by the Belgian Companies and Associations' Code (the ***BCAC***)), an NPO is managed and represented towards third parties by the board of directors. All powers that were not explicitly allocated by law to the shareholders' meeting are considered to form part of the powers of the board of directors.

The Supreme Court reasoned that even if the NPO is managed by a collegial board of directors, each individual director has a duty to supervise the fellow directors. This duty is not affected by any internal division of tasks amongst the directors, by the fact that a director did not actively seek his or her mandate as a director or by the fact that the director did not actively perform his or her mandate.

On that basis, the Supreme Court overturned the judgment of the Court of Appeal and held that the defendant could not escape her joint directors' liability by arguing that she had not had an active involvement in the fault at hand or the management of the NPO in general.

The NPO Law was replaced by the BCAC in 2019. However, the duty of supervision is based on the collegial character of the board of directors and it is therefore expected that that duty continues to apply under the BCAC to both commercial companies and NPOs.

DATA PROTECTION

Court of Justice of European Union Confirms Indiscriminate Access and Retention of Traffic and Location Data to be Unlawful

On 6 October 2020, the Court of Justice of the European Union (the ***CJEU***) delivered judgments in three cases regarding the compatibility of specific methods for combating terrorism with Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the ***ePrivacy Directive***) (Case C-623/17, *Privacy International;* Joined cases C-511/18, *La Quadrature du Net and Others* and C-512/18, *French Data Network and Others*; and Case C-520/18, *Ordre des barreaux francophones et germanophone and Others*).

In these cases, various prejudicial questions had been referred to the CJEU on the retention of traffic and location data and the transmission of such data to public authorities for national security and other purposes. After the CJEU had prohibited "general and indiscriminate" retention obligations and invalidated Data Retention Directive 2006/24/EC (*See, this Newsletter, Volume 2014, No. 4, p. 13*), Member States were deprived of an instrument which they consider necessary to safeguard national security and to combat crime and terrorism. They therefore proceeded to create a similar instrument. The new rules were again called into question by privacy advocates. This led to new preliminary questions being referred to the CJEU by the UK Investigatory Powers Tribunal, the Belgian Constitutional Court (*Grondwettelijk Hof / Cour constitutionnelle*) and the French Council of State (*Conseil d'Etat*).

In its answer to these questions, the CJEU confirmed once again that EU law prevents national legislators from imposing broad obligations on providers of electronic communications services to retain or transmit traffic and location data. However, the CJEU judgments also provide guidance on which retention and transmission requirements can be considered to be compatible with EU law and how national criminal courts should handle evidence that is collected on the basis of illegal retention and transmission requirements. The judgments are largely in line with the opinion which the Advocate General gave in these cases (*See, this Newsletter, Volume 2020, No. 1, at p. 9*).

As a result of these judgments, Member States must review their legislation and practices for compliance with EU requirements to protect the public, its security and fundamental rights. In addition, the judgments could have an impact on EU-UK personal data transfers post-Brexit.

Privacy International Case

Privacy International, a non-governmental organisation, brought an action before the UK Investigatory Powers Tribunal challenging the UK security and intelligence agencies' (***SIAs***) collection and use of bulk personal data, including communications data acquired from providers of public electronic communications networks. Privacy International's claim is based on the CJEU judgment in Case C-698/15, *Tele2 Sverige and Watson and Others* (*See, this Newsletter, Volume 2017, No. 1, p. 14*). In this 2016 judgment, the CJEU held that the general and indiscriminate retention of all traffic and location data of all subscribers and registered users is disproportionate and incompatible with EU law.

In the *Privacy International* case, the CJEU first determined that a requirement in national legislation for communications service providers to retain data falls within the scope of the ePrivacy Directive. This is because Article 3 of the e-Privacy Directive makes it clear that the Directive applies to the activities of communications service providers, and laws requiring communication service providers to retain and transmit traffic and location data are caught by Article 15 of the ePrivacy Directive. Such practices "*necessarily involve the processing, by those providers, of the data and cannot, to the extent that they regulate the activities of those providers, be regarded as activities characteristic of States*". A legislative measure such as section 94 of the UK Communications Act, based on which the competent authority may give the providers of electronic communications services a direction to disclose bulk data to the SIAs, thus falls within the scope of the ePrivacy Directive. The CJEU thus rejected the argument that these rules concern public security and therefore fall outside the scope of EU law.

Second, the CJEU pointed out that the purpose of the ePrivacy Directive is to protect users from threats to their privacy arising from new technologies. It thus gave expression to Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (the ***Charter***). However, Article 15(1) of the ePrivacy Directive allows Member States to adopt restrictions to specific rights, provided that such restrictions are "*necessary, appropriate and proportionate*". The CJEU cautioned that the exceptions to the obligation to ensure the confidentiality of electronic communications could not be defined so broadly that they would effectively become the rule. This also applies to the prohibition on keeping data longer than necessary for their initial purpose. Restrictions to these fundamental rights must comply with the Charter. Referring to *Schrems II* (*See, this Newsletter, Volume 2020, No. 7, at p. 8*), the CJEU held that any limitation on the exercise of fundamental rights must be provided for by law. This implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned.

Derogations from the protection of personal data and any restriction on confidentiality of communications and traffic data must thus be proportionate, meaning that they may apply only in so far as is *strictly* necessary and while "*properly balancing the objective of general interest against the rights at issue*". Proportionality also requires the legislation to lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards to protect against the risk of abuse. The legislation must ensure that interference with the protection of personal data is limited to what is "strictly necessary". "*Necessity*" means that due account should be taken of the risk at hand. The CJEU pointed out that automated processing gives rise to more significant risks and added that all of its considerations are more pressing for sensitive data.

The CJEU noted that the transmission of data to SIAs constituted a breach of confidentiality in a general and indiscriminate way. The broad scope of this exception makes disclosure – and not confidentiality – the rule.

Finally, the CJEU distinguished between various objectives set out in the ePrivacy Directive. The importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU, goes beyond that of the other objectives referred to in Article 15(1) of the ePrivacy Directive (*i.e.,* the objectives of combating crime in general, even serious crime, and of safeguarding public security). While measures safeguarding national security must still comply with Article 52(1) of the Charter, the CJEU considered that the seriousness of threats comprising "national" security are, in principle, capable of justifying more intrusive measures on fundamental rights than those which might be justified by the other objectives foreseen in Article 15(1) of the ePrivacy Directive.

On this basis, the CJEU held that national legislation requiring providers of electronic communications services to disclose traffic data and location data to the SIAs through general and indiscriminate transmission exceeds the limits of what is strictly necessary. This requirement cannot be justified within a democratic society, even in the interests of protecting national security.

The full text of the CJEU's judgment can be found here (in English).

Joined Cases La Quadrature du Net and Ordre des barreaux francophones et germanophone

The joined cases C-511/18, C-512/18 and C-520/18, concern, first, actions brought by *La Quadrature du Net and Others* before the Council of State in France to challenge a French decree related to specialised intelligence services. There are, second, actions initiated by the *Ordre des barreaux francophones et germanophone and Others* before the Constitutional Court of Belgium to challenge Belgium's legislation governing collection and retention of communications data. In particular, the French court asked questions about the collection of live traffic and location data while the Belgian court sought guidance on the use of data obtained in breach of EU law during criminal proceedings. Since the cases raised similar questions, the CJEU decided to join them.

In response to the questions raised by the French and Belgian courts on the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies with the goal of safeguarding national security, the CJEU adopted the same reasoning as it espoused in the *Privacy International case*. It held that national legislation requiring such measures was precluded under the Charter and Article 15 of the ePrivacy Directive.

In addition, the Belgian and French courts asked the CJEU for clarification on the criteria and purposes for which national law could require traffic and location data to be retained.

The CJEU considered that neither the ePrivacy Directive nor the Charter precludes recourse to an order requiring providers of electronic communications services to retain, generally and indiscriminately, traffic data and location data. This is, however, only the case when the Member State at issue is facing a sufficiently serious threat to national security (i.e., a threat that is genuine and actual or foreseeable). In such a case, data retention must be proportionate, and the retention can only be for a period limited to what is strictly necessary. If such an order is renewed, it must be for a specified length of time. Additionally, the retained data must be protected by precise safeguards against the risk of abuse. Finally, the CJEU explained that the decision must be subject to effective review by an independent body whose decision is binding. Again, the CJEU pointed out that the objective of safeguarding national security is capable of justifying measures entailing more serious interferences with fundamental rights than those that might be justified by the objectives foreseen in Article 15(1) of the ePrivacy Directive.

By contrast, the CJEU observed that the concept of general and indiscriminate surveillance refers to a measure which covers virtually the entire population without any differentiation, limitation or exception in the light of the objective pursued. It therefore even applies to persons with respect to whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with the objective of combating serious crime and, in particular, without there being any relationship between the data whose retention is provided for and the threat to public security.

The CJEU then addressed the issue whether national law could require the retention of IP addresses and data relating to the civil identity of users of electronic communication systems. The CJEU held that IP addresses could be retained as a precautionary measure in a general and indiscriminate manner, subject to a requirement of strict necessity. Further, it considered the different purposes for which identification of users of electronic communication systems could be relevant and held that the ePrivacy Directive does not preclude the retention of data beyond statutory data retention periods when strictly necessary to shed light on serious criminal offences or attacks on national security, or when the offences or attacks have already been established, or if their existence may reasonably be suspected.

Moreover, the CJEU stated that real-time data could be used, for instance when it is limited to people in respect of whom there is a valid reason to suppose that they are involved in terrorist activities. However, the use of such data must be subject to prior review by an independent body to ensure that real-time collection is limited to what is strictly necessary. The CJEU noted that in urgent cases that review should take place promptly.

Finally, the CJEU provided guidance on the legal consequences of the invalidation of national data retention rules. In a statement that may be relevant for many pending cases, the CJEU noted that the use of evidence obtained on the basis of retention rules that were declared to be illegal could affect the right of a fair trial. Therefore, it held that national criminal courts should "*disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law*" if the suspect is not in a position to defend himself or herself against such data effectively and this could have a significant impact on the case.

The full text of the CJEU's judgment can be found here (in English).

Impact of judgments on EU-UK personal data data flows

The UK officially left the EU on 31 January 2020 and there is a transition period until the end of 2020 to allow for time to negotiate a new relationship with the EU. During this transition period, EU law continues to apply to the UK. Following the transition period, there will be a need for a new regulatory framework governing data transfers between the EU and the UK. From the EU's perspective, the UK will be a third country. The GDPR contains the possibility for the European Commission to adopt an adequacy decision which would facilitate such transfers. If such a decision involving the UK were adopted, the European Commission would recognise that UK legislation ensures a high level of data protection that is at least similar to the level offered by the GDPR. As a result, personal data would move freely between the EU and UK.

While it is generally expected that UK legislation, which copied the substantive provisions of the GDPR, should qualify for an adequacy finding, the above CJEU judgments suggest that such a decision may still not be straightforward. UK surveillance law and its provisions for the collection of bulk communications data will have to be assessed by the European Commission in the light of these judgments. In the absence of an adequacy finding, organisations transferring personal data between the UK and the EU may be required to resort to other means to bring such transfers in line with the GDPR.

Belgian Data Protection Authority Penalises Use of Former Employees' E-mail Addresses After Dismissal

On 29 September 2020, the Litigation Chamber (*Geschillenkamer/Chambre contentieuse* – the ***Litigation Chamber***) of the Belgian Data Protection Authority (*Gegevensbeschermingsautoriteit/Autorité de protection des données* – the ***DPA***) imposed a fine of EUR 15,000 on a company for continuing to use the e-mail addresses of its employees after their departure from the company.

Factual Background

In November 2016, a company active in the medical devices sector (the ***company***) decided to dismiss its managing director (the ***claimant***). In March 2019, the claimant noticed that his e-mail address (and those of members of his family who had also left the company) remained active. As a result, he requested the company to stop using those e-mail addresses. When the company failed to heed the request, he filed a complaint with the DPA. After a failed mediation initiated by the parties, the case was transferred to the DPA's Litigation Chamber.

Purpose Limitation, Data Minimisation and Storage Limitation

The Litigation Chamber considered that the e-mail addresses, whether they contain the surname and first name or only the first name of the person to whom they have been attributed, are personal data in that they constitute information relating to identified or identifiable persons within the meaning of Article 4.1 of the General Data Protection Regulation (the ***GDPR***).

Under the principle of purpose limitation set out in Article 5.1 (b) of the GDPR, personal data must be collected for specified, explicit and legitimate purposes. In addition, pursuant to Article 5.1 (c) and (e), the data collected must be adequate, relevant and necessary in relation to the purpose for which they are processed (principle of data minimisation) and kept in a form that permits identification of data subjects for no longer than is necessary in relation to that purpose (principle of storage limitation). In that respect, the company argued that the purpose of the use of the e-mail addresses after the departure of the employees was to avoid losing important professional communications and to ensure the transmission of files and the reception of messages from national regulatory bodies active in the medical devices sector.

However, the Litigation Chamber considered that in order to comply with the principle of purpose limitation, combined with the principle of data minimisation and the principle of storage limitation, the data controller must block the electronic mailboxes of former employees who have left the company at the latest on the day of their actual departure and after informing them of the closure. This solution should prevail over automatic transfers of the former employees' e-mails to another e-mail address, which prevent any type of control of incoming e-mails and increase the risk of disclosure of sensitive private information.

The Litigation Chamber also held that before blocking the mailbox, the company must insert an automatic e-mail in order to (i) warn future correspondents that the holder of the e-mail address is no longer part of the company; and (ii) provide the contact details of the person to be contacted in his place during a reasonable period of time of around one month. This period of time can be extended to no longer than three months, depending on the degree of responsibility of the former employee and provided this extension is justified and decided in agreement with the former employee (or at least following a notification of the former employee). Beyond that period of time, the mailbox must be deleted.

Consequently, in the case at hand, the company was found to be in breach of Article 5.1 (b) combined with Article 5.1 (c) and (e) of the GDPR because it should have (i) blocked the mailboxes of its former employees on the day of their departure and informed them of this blocking, (ii) informed the correspondents of the employees' departure with an automatic response, and (iii) deleted the mailboxes within a reasonable period of time.

Lawfulness of Processing

The processing of personal data must be based on one of the legal bases set out in Article 6 of the GDPR. The Litigation Chamber noted that maintaining the e-mail addresses active for a reasonable period of time after the employees' departure in order to ensure the proper functioning of the company and the continuity of its activities constitutes a legitimate interest within the meaning of Article 6.1 (f) of the GDPR. By contrast, beyond that reasonable period of time, the Litigation Chamber considered that there was no legal basis allowing for the processing to continue. As a result, keeping the mailboxes active during a longer period was also found to be in breach of Article 6 of the GDPR.

Right to Erasure

In addition to the obligations which they impose on data controllers, the principles of purpose limitation, data minimisation and storage limitation entail rights for data subjects. Pursuant to Article 17. 1 (a) of the GDPR, data subjects may request the data controller to erase their personal data when such data are no longer necessary for the purposes for which they were collected or processed. Under Article 12.3 of the GDPR, data controllers must respond to this request within one month. In the case at hand, the company was found to have violated Article 17.1 (a) of the GDPR combined with Article 12.3 of the GDPR in that it had failed to respond to the complainant's request to deactivate the e-mail addresses.

Sorting of Private and Professional E-mails

Furthermore, the Litigation Chamber considered that a data subject must be able to erase his or her private electronic communications before the mailbox is blocked. If it is necessary to ensure the smooth functioning of the company, the recovery of a part of the employee's mailbox must be done prior to the employee's departure and in his or her presence. A trustworthy person must become involved in the event of a dispute. The Litigation Chamber also stressed the importance of establishing a clear internal policy on the use of IT resources in case of an employee's departure.

Given the various infringements that were established, the Litigation Chamber decided to impose an administrative fine of EUR 15,000.

The DPA decision is currently only available in French here.

Belgian Data Protection Authority Publishes 2019 Annual Report

On 30 September 2020, the Belgian Data Protection Authority (*Gegevensbeschermingsautoriteit/Autorité de protection des données* - the ***DPA***) published its Annual Report for 2019 (the ***Report***).

2019 Developments and Accomplishments

1. The DPA published its strategic plan for 2020-2025 which sets out the DPA's vision, priorities and strategic objectives for the coming years and identifies the resources needed to guide organisations and citizens towards a digital world where privacy is considered a reality for all (*See, this Newsletter, Volume 2019, No. 12, p. 7*).

2. The DPA imposed its first fines under the General Data Protection Regulation (the ***GDPR***). In May 2019, the DPA imposed a first fine of 2,000 EUR on a mayor who had misused, for political publicity, e-mail addresses obtained during his term of office (*See, this Newsletter, Volume 2019, No. 5, p. 12*). Another important financial sanction in 2019 concerned the non-compliance of a website with the provisions concerning the use of cookies (*See, this Newsletter, Volume 2020, No. 1, p. 10*).

3. A proactive monitoring system for technological and societal evolutions related to privacy and data protection was implemented. The monitoring system allows the DPA to respond rapidly to processing activities that could infringe the rights and freedoms of data subjects.

4. Several initiatives were adopted to raise awareness about data protection and privacy, specifically for vulnerable data subjects. Initiatives include a toolbox for SMEs to support them in the implementation of the GDPR and platforms for private individuals such as "beschermjegegevens.be/ maitrisermesdonnees.be" and "Ik beslis / je decide".

2019 in Numbers

1. During the past year, the DPA dealt with a total of 6,447 cases. This includes 5,168 requests for information and 331 requests for mediation or complaints. The requests for information and mediation mostly related to general questions about the GDPR, data subjects' rights and privacy principles, the use of surveillance cameras, the right to image, and direct marketing.

2. According to the DPA, the amount of cases relating to data breaches has "exploded", showing an increase of 95.82% (from 445 notifications in 2018 to 869 in 2019). This is attributed to the fact that the obligation to notify data breaches became a general obligation in the middle of 2018 (prior to this, the notification requirement only applied to the telecommunications sector).

3. Since 25 May 2018, 4,908 data protection officers have notified their position to the DPA.

Resolutions for 2020

For the remainder of 2020, the DPA promises to continue its efforts towards raising data protection and privacy awareness. Faced with the many challenges that the current Covid-19 pandemic poses for data protection, the DPA has created a separate platform to raise awareness, provide guidelines and answer FAQs (this is available here). In the context of the current health crisis, the DPA provided advice on legislation concerning contact tracing and closely monitored other initiatives, such as the installation of 'intelligent cameras' at the Belgian coast to monitor the influx of people, temperature measurement at Brussels Airport, and the way customers' data is collected and used by restaurants and bars.

The full annual report can be consulted in Dutch and in French.

Belgian Data Protection Authority Publishes Frequently Asked Questions for Small and Medium-sized Enterprises

On 1 October 2020, the Belgian Data Protection Authority (*Gegevensbeschermingsautoriteit/Autorité de protection des données* - the ***DPA***) published Frequently Asked Questions (***FAQ***) to assist small and medium-sized enterprises (***SMEs***) regarding their obligations under the General Data Protection Regulation (***GDPR***). The FAQ do not deal with all aspects of the GDPR but focus on the significant issues such as when an SME acts as a controller or processor and whether an SME should hire a Data Protection Officer.

For example, the FAQ address the issue of whether the GDPR applies to SMEs. To this end, the FAQ explain the scope of the GDPR and provide two examples of when a commercial enterprise or a non-profit organisation falls within the scope of the GDPR and must thus comply with the obligations under the GDPR. Further, the FAQ also offer concrete tips to assist SMEs with their obligations under the GDPR. For example, regarding the preparation and communication of a privacy notice, the FAQ contain a checklist for SMEs. According to the checklist, a privacy statement must include the purpose of the processing, the retention period of the personal data and the precise rights of the person concerned.

The FAQ can be accessed in Dutch and in French.

European Data Protection Board Guidelines on Other Supervisory Authorities' Relevant and Reasoned Objection under Article 60 of the GDPR

On 8 October 2020, the European Data Protection Board (***EDPB***) adopted guidelines on the notion of relevant and reasoned objection under the General Data Protection Regulation (the ***GDPR***; hereinafter the ***Guidelines***). The Guidelines aim to establish a common understanding of the notion "relevant and reasoned opinion" pursuant to Article 60 of the GDPR, which sets out the "one-stop-shop" mechanism. That mechanism was introduced by the GDPR to ensure cooperation between the lead supervisory authority (***LSA***) and other relevant supervisory authorities. It is mainly relevant for organisations active in different EU Member States.

For companies conducting cross-border data processing, the LSA will be identified on the basis of the determining location of the controller's main establishment or single establishment. The LSA will ensure enforcement of the applicable data protection laws and will provide guidance. When an infringement of the GDPR occurs, the case may be handled by the LSA only, or by the LSA in cooperation with other supervisory authorities. The one-stop-shop mechanism exists to ensure that cross-border privacy related issues are addressed consistently across the EU.

Under the cooperation mechanism created by the GDPR, the supervisory authorities have a duty to exchange all relevant information with each other and a duty to cooperate in an endeavour to reach consensus (Article 60(1) of the GDPR). The ultimate goal of the procedure established by Article 60 of the GDPR is to achieve an agreement on the outcome of the case. If no consensus is reached among the supervisory authorities, Article 65 of the GDPR entrusts the EDPB with the power to adopt binding decisions.

In accordance with Article 60(3) of the GDPR, the LSA is required to submit a draft decision to the other supervisory authorities concerned, which then may raise a relevant and reasoned objection within a timeframe of four weeks. Upon receipt of a relevant and reasoned objection, the LSA has two options. First, if the LSA does not follow the relevant and reasoned objection, the LSA will submit the matter to the EDPB in accordance with the consistency mechanism under Article 65 of the GDPR. By contrast, if the LSA follows the objection and issues a revised draft decision, the concerned supervisory authorities may again express a relevant and reasoned objection on the revised draft decision within two weeks.

The Guidelines are available here. They are open for public consultation until 24 November 2020.

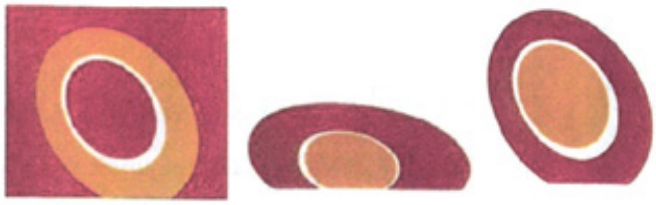
INTELLECTUAL PROPERTY

Court of Justice of European Union Rules on Distinctiveness of Trade Marks Applied to Busses and Trains

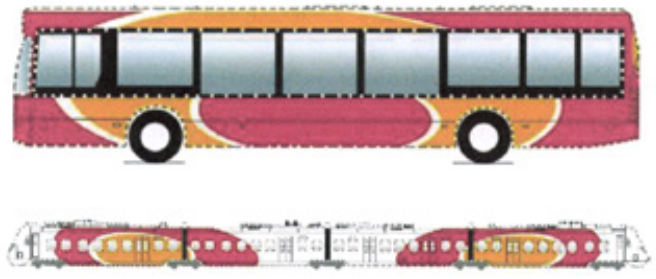
On 8 October 2020, the Court of Justice of the European Union (***CJEU***) delivered an interesting view on distinctiveness of a trade mark in its judgment in case *Aktiebolaget Östgötatrafiken v Patent-och registreringsverket* (case C-456/19). The CJEU held that the assessment of the distinctiveness of a sign applied to specific goods should not always take into consideration the norms and customs of the relevant economic sector.

Factual Background and Procedure

In November 2016, Östgötatrafiken applied to register several figurative signs, including the figures below, as Swedish trade marks for various services provided by means of vehicles and transport in Class 39. The full set of images in the application can be viewed in the CJEU judgment which is available here.



The applications also included drawings of busses and trains with the design applied. However, the protection applied for did not relate to the shape of the vehicles.



The applications were rejected by the Swedish Patent and Registration Office on the ground that the signs are merely decorative and cannot be perceived as capable of distinguishing the services covered by the applications.

Östgötatrafiken appealed to the Swedish Patent and Market Court, which dismissed the action by stating that it could not be established that the colours and shape of the signs departed significantly from the way other companies decorate their vehicles. Östgötatrafiken further appealed to the Swedish Patent and Market Court of Appeal, which stayed the proceedings and referred the matter to the CJEU for a preliminary ruling.

Judgment

The CJEU considered existing case law under Directive 2015/2436 (***Trade Mark Directive***), which applies the criterion of a "significant departure from the norm or customs of the sector" in cases where the sign consists in the appearance of the product itself. In such cases, the case law also takes account of the perception of the relevant public, namely the average consumer of the category of goods or services in question (*Henkel v. OHIM* (C-456/01 and C-457/01), *Storck v. OHIM* (C-25/05), *Voss of Norway v. OHIM* (C-445/13).

The CJEU maintained that if a trade mark application concerns a sign that is intended to be attached exclusively and systematically in a specific way to a large part of the goods used to provide the services, the distinctive character of that sign cannot be assessed independently of the perception of the relevant public of the attachment of that sign, even if the goods which are used to provide the services are not the subject of the trade mark application.

Under the Trade Mark Directive, the criterion for assessment of whether there is a significant departure from the norm or customs of the concerned economic sector applies where the sign consists of the shape of the product for which registration as a trade mark is sought. It also applies where the sign consists of the representation of the layout of the spatial environment in which the services in respect of which registration as a trade mark is sought are provided (Apple, C-421/13). However, at the same time, the CJEU clarified that this criterion does not always apply.

For instance, the CJEU explained that this situation would not arise in a case like the one at hand because the signs consist of colour compositions which are systematically arranged and spatially limited. Moreover, their purpose is not to represent the spatial environment in which the services are provided. Therefore, the distinctiveness of the signs in question must be assessed by considering the perception of the relevant public, and it is not necessary to examine whether this constitutes a significant departure from the norm or customs of the relevant economic sector.

EU's General Court Holds That Brexit Will Not Affect Protection Granted to Older EU Trade Marks

On 23 September 2020, the General Court (***GC***) delivered its judgment in *Bauer Radio Ltd v European Union Intellectual Property Office* (Case T-421/18) and held that the withdrawal of the United Kingdom (***UK***) from the European Union (***EU***) will not affect the protection granted to earlier EU trade marks.

Factual Background and Procedure

In November 2013 Simon Weinstein, an Austrian national, submitted an EU trade mark application to the European Union Intellectual Property Office (***EUIPO***) for the word sign MUSIKISS for services in Classes 35, 41 and 45.

In May 2014, Bauer Radio filed an opposition to the registration of the trade mark and referred to the earlier word and figurative marks KISS registered in the UK. Bauer Radio claimed that the earlier marks are distinctive and have a reputation in the UK in respect of all the goods and services covered by those marks. As the application relates to similar signs, Bauer Radio argued that the application should be refused on the basis of Article 8(1)(b) and Article 8(5) of Regulation No 207/2009 (now Article 8(1)(b) and Article 8(5) of Regulation 2017/1001 on the European Union Trade Mark).

In 2017, the Opposition Division upheld the opposition in part, but allowed the registration in respect of the services in Class 35. Mr. Weinstein appealed to the EUIPO and Bauer Radio filed an ancillary appeal against the Opposition Division's decision.

In March 2018, the First Board of Appeal of EUIPO (***Board of Appeal***) annulled the Opposition Division's decision and referred the case back to the Opposition Division for further examination. Bauer Radio further appealed to the GC.

Judgment

The GC dismissed Bauer Radio's appeal and made several interesting observations.

The GC first noted that the Withdrawal Agreement, which sets out the arrangements for the withdrawal of the UK from the European Union, entered into force on 1 February 2020 and provides for a transition period from 1 February to 31 December 2020, which may be extended once for a maximum duration of two years (***Transition Period***). Moreover, Article 127 of the Withdrawal Agreement stipulates that EU law continues to apply in the UK during the Transition Period, unless provided otherwise. Therefore, Regulation 2017/1001 on the European Union trade mark continues to apply to UK trade marks until the end of the Transition Period so that the earlier marks registered by the applicant in the UK continue to receive the same protection as they would have received had the UK not withdrawn from the EU.

The GC added that the fact that the earlier trade mark could lose the status of a trade mark registered in a Member State at a time after the filing of the application for registration of the EU trade mark is irrelevant to the outcome of the opposition.

The GC concluded that the withdrawal of the UK from the EU has no impact on the protection granted to earlier EU trade marks. Accordingly, those trade marks can still form the basis of an opposition to registration of the mark applied for.

The judgment of the GC can be consulted here.

LABOUR LAW

Covid-19: Overview of Recent Government Measures That Impact Employment

Pursuant to the Ministerial Decree of 18 October 2020 (*Ministerieel Besluit houdende dringende maatregelen om de verspreiding van het coronavirus COVID-19 te beperken / Arrêté ministériel portant des mesures d'urgence pour limiter la propagation du coronavirus COVID-19* - the ***Ministerial Decree***), a number of new measures were implemented in order to limit the further spreading of the COVID-19 virus. The Ministerial Decree entered into force on 19 October 2020 (the rules governing the curfew entered into force on 20 October 2020).

Based on the Ministerial Decree (i) all restaurants and bars had to be closed; (ii) teleworking again became the norm, and (iii) a curfew applied between 12 am and 5 am.

The measures were to apply until 19 November 2020 but have been extended in the meantime until at least 13 December 2020.

The most important effects on Belgian employers are as follows.

Temporary Unemployment – Simplified Procedure

At the beginning of the COVID-19 pandemic two temporary unemployment schemes were adopted that allow employers to suspend the employment contract of their employees and suspend their payment obligations (*See, VBB Article of 19 March 2020*). These are:

- the temporary unemployment regime because of *force majeure*; and
- the temporary unemployment regime for economic reasons.

Initially and applicable as from 13 March 2020, because of the COVID-19 pandemic, the formalities for applying temporary unemployment for reasons of *force majeure* were reduced significantly. Any employer who suffered from the consequences of COVID-19 could invoke temporary unemployment for *force majeure*.

However, as from 1 September 2020, the possibility to apply this simplified regime was restricted to entities earmarked as "particularly impacted" by the pandemic, such as firms belonging to the hospitality industry.

The full list of sectors that are particularly impacted can be found here (pages 66844 and 66845). The list makes a distinction between:

- Joint Committees (*Paritair Comité/Commission Paritaire*) which are considered to be impacted in their entirety (Joint Committee Nos. 140.02, 227, 302, 303.03, 304, 329 and 333); and
- Joint Committees for which only specific activities are considered as particularly impacted (Nos. 100, 109, 111, 126, 139, 140.01, 140.04, 149.01, 200, 209, 215, 226, 314 and 315).

If a firm did not belong to any of these lists, it could still apply the regime of temporary unemployment for reasons of *force majeure* subject to a number of conditions: it had to demonstrate at least 20% of temporary unemployment days in the second quarter of 2020 due to a lack of work for economic reasons or for *force majeure* as compared to the overall number of workings days communicated to the National Social Security Office (*Rijksdienst voor Sociale Zekerheid / Office National de Sécurité Social*).

Finally, if none of the above conditions prevailed, a firm could still apply the regime of temporary unemployment for economic reasons subject to several other conditions (*See, VBB Article of 19 March 2020*).

On 6 November 2020, the federal government decided to reinstate the simplified temporary unemployment for reasons of *force majeure* due to COVID-19. It did so retroactively starting on 1 October 2020 and the new regime will apply until 31 March 2021. As a result, any employer who suffers from the consequences of COVID-19 can apply temporary unemployment on grounds of *force majeure*.

Teleworking and Compliance with Social Distancing Measures

In accordance with the Ministerial Decree, teleworking should again be the rule for all jobs for which this is possible and to the extent it allows the continuity of the business of the firm.

If telework is not applied (*e.g.* for certain functions for which this is not possible), the employer must take sufficient measures to ensure maximum compliance with the social distancing rules and the rules intended to prevent COVID-19 contamination. The general (click here) and sectoral guidelines (click here) should be observed.

In a nutshell, the basic principles are as follows:

- Collective employment measures must prevail over individual measures;
- Firms must adopt the necessary health and safety measures in due time in order to provide the maximum level of protection;
- The measures must be drawn up at company level, with the involvement of employees' representatives or in consultation with the employees concerned and in consultation with the services for prevention and protection at work; and
- Employees must receive appropriate training.

Curfew and Employer's Certificate

The Ministerial Decree establishes a curfew between 12.00 am and 5.00 am in order to minimise gatherings, parties and alcohol consumption in public. However, the curfew does not apply to essential travel that cannot be postponed, such as travel to seek medical care or travel for professional purposes. Employers should provide staff with a certificate stating that teleworking is not possible and professional travels are necessary.

The Ministerial Decree specifies that, except for urgent medical reasons, the reason for presence or movement in public should be justified at the first request to the police.

The Walloon and Brussels Governments expanded the curfew to the period between 10.00 pm and 6.00 am.

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