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

Legal 500 2019

March 2021

# 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

***Belgian Competition Authority Publishes Enforcement Priorities for 2021***

On 10 March 2021, the Belgian Competition Authority (*Belgische Mededingingsautoriteit / Autorité belge de la Concurrence* - ***BCA***) published its list of enforcement priorities for 2021 (*See*, website of BCA, in Dutch and in French).

The document discusses the impact of the Covid-19 pandemic on the Belgian economy and stresses the importance of fair competition, both in sectors that were hit hard by the crisis and in sectors where the pandemic created new opportunities.

The BCA identifies three "strategic priorities" that apply across industries: (i) digital platforms; (ii) the enforcement of the new prohibition of abuse of economic dependence, which entered into force on 22 August 2020 (*See*, this Newsletter, Volume 2020, No. 8, p. 4); and (iii) the enforcement of the competition rules to boost the Belgian green and circular economy.

The rest of the document lists the economic sectors in which the BCA considers the enforcement of the competition rules to be a priority. These priorities form, by and large, a continuation of the priorities that applied in 2020 (*See*, this Newsletter, Volume 2020, No. 3, p. 6).

- The telecommunications sector fell from its first position in 2020 to the last position in the BCA's list of priorities this year. The top position is now occupied by the digital economy (which had the sixth position out of seven in 2020). The BCA notes that several initiatives are underway, such as the Digital Services Act and the Digital Markets Act published by the European Commission in December 2020, as well as measures taken at the national level. The BCA announces that it will "*help to ensure that the implementation of these measures and the cooperation between the various authorities and the European Commission are as efficient and successful as possible*".
- The second priority sector for 2021 is that of the "*services to business and to consumers (in particular regulated professions)*", which moved up one place from its third position in 2020. Legal, accounting, architecture and engineering services are mentioned, as well as those provided by real estate agents.
- The retail sector continues to be in the BCA spotlight, with a third position in the BCA's priorities for 2021 (down one place compared to 2020). As in previous years, the BCA expresses concern over the Belgian pricing level of consumer goods, including foodstuffs, which exceeds that of neighbouring countries. Additionally, the BCA notes that prices for both unprocessed and processed foodstuffs have increased more rapidly than the rate of inflation.
- The energy sector (fourth position) is a newcomer in the 2021 list compared to the BCA's enforcement priorities for 2020. The BCA wants to ensure that the phasing out of nuclear power does not lead to anticompetitive collusion between the remaining market players.
- The pharmaceutical sector already featured on the BCA's list in 2020, at the same (fifth) position. The BCA notes that the Covid-19 pandemic showed the importance of this sector and intends to monitor all levels of the supply and distribution chain.
- The logistics (sixth position in 2021, one place up from its seventh position in 2020) and public procurement sectors (seventh position in 2021; fourth position in 2020) remain among the BCA's priorities.
- The telecommunications sector is the eighth and final one to feature on the BCA's priority list for 2021, dropping from the first position in 2020.

***Adoption of Draft Bill to Exclude Clinical Networking between Hospitals from Application of Merger Control***

On 18 March 2021, the federal Chamber of Representatives adopted a bill seeking to exclude the creation of local hospital networks (*locoregionaal ziekenhuisnetwerk / réseau hospitalier locorégional*) and any subsequent change in their composition from the application of the Belgian merger control rules by the Belgian Competition Authority (*Belgische Mededingingsautoriteit / Autorité belge de la Concurrence*) (*See*, this Newsletter, Volume 2021, No. 2, p. 7).

The Law of 29 March 2021 was published in the Belgian Official Journal (*Belgisch Staatsblad / Moniteur belge*) on 16 April 2021 (*Wet van 29 maart 2021 tot wijziging van de gecoördineerde wet van 10 juli 2008 op de ziekenhuizen en andere verzorgingsinrichtingen, wat de toepassing van de voorafgaande controle op concentraties van de klinische netwerking tussen ziekenhuizen betreft/Loi du 29 mars 2021 modifiant la loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soins, en ce qui concerne l'application du contrôle préalable des concentrations pour le réseautage clinique entre hôpitaux*).

***Belgian Competition Authority Imposes New Fine on Professional Organisation of Pharmacists***

On 26 March 2021, the Belgian Competition Authority (*Belgische Mededingingsautoriteit / Autorité belge de la Concurrence* - ***BCA***) announced that its Competition College (*Mededingingscollege / Collège de la Concurrence*) had imposed a fine of EUR 245,000 on the professional organisation of pharmacists (*Orde der Apothekers / Ordre des pharmaciens* - the ***PO***) on account of an anticompetitive agreement contrary to Article IV.1 of the Belgian Code on Economic Law (***CEL***) and Article 101 of the Treaty on the Functioning of the European Union (***TFEU***).

This fine replaces a higher fine already imposed on the PO for the same infringement. In a decision of 28 May 2019, the BCA found that the PO had taken a range of exclusionary measures to thwart the development of MediCare-Market, a retailer of medicines and other health products, and thus imposed a fine of EUR 1 million on the PO (*See*, this Newsletter, Volume 2019, No. 6, p. 3).

However, on 8 January 2020, the Markets Court (*Marktenhof / Cour des marchés*) of the Brussels Court of Appeal held that the BCA had misapplied the rules on the calculation of fines. Fines cannot exceed 10% of the turnover of the undertaking or (in this case) of the association of undertakings concerned. The BCA applied this cap by adding up the turnover of the members of the PO. The Markets Court found that the version of Book IV CEL in force in May 2019 did not allow for this approach. As a result, while the Markets Court confirmed that the PO had infringed Articles IV.1 CEL and 101 TFEU, it annulled the fine and referred the case back to the BCA for a recalculation of the fine. It was estimated at the time that the fine eventually imposed by the BCA would be reduced to around EUR 250,000 (*See*, this Newsletter, Volume 2020, No. 1, p. 5). The new fine of EUR 245,000 reflects that expectation.

Book IV of the CEL was modified in May 2019. The current version of Book IV of the CEL allows the BCA to calculate the fine cap of 10% on associations of undertakings based on "*the total of the turnover of all the active members on the relevant market*". Associations of undertakings therefore now run the risk of much higher fines for an infringement of the competition rules than the fine which the PO eventually received in this case.

***European Commission Issues Notice on Tools to Fight Collusion in Public Procurement***

On 18 March 2021, the Official Journal of the European Union published a European Commission (***Commission***) Notice on "*tools to fight collusion in public procurement and on guidance on how to apply the related exclusion ground*" (the ***Notice***; available here). The Notice develops the tools which the Commission announced in its Communication COM(2017) 572 entitled "*Making public procurement work in and for Europe*" (available here) with a view to assisting EU Member States and their contracting authorities in tackling collusion in public procurement.

The Notice provides guidance on how:

1. EU Member States and contracting authorities can deter, detect and address collusion in public procurement (*See*, Section 3);

2. cooperation between national central procurement (***NCP***) and competition authorities can be improved – NCP refers to the authority entrusted with drawing up, implementing, monitoring and/or supporting the functioning of the public procurement regulatory framework at national level (*See*, Section 4); and

3. contracting authorities should apply the collusion-related exclusion ground provided for in the EU public procurement Directives (*See*, Section 5).

The Notice is accompanied by an Annex which provides pointers for contracting authorities on how to (i) design award procedures in a way that deters collusion between tenderers; (ii) detect potential collusion when evaluating tenders; and (iii) react to such suspected collusion.

Collusion in public procurement has been high on the agenda of competition authorities in recent years and is set to remain so over the next years. For example, the Belgian Competition Authority (***BCA***) signalled its determination to tackle anticompetitive behaviour in public procurement proceedings by publishing a 34-page guide on bid rigging in January 2017 (*See*, this Newsletter, Volume 2017, No. 1, p. 8). Similarly, in the BCA's list of enforcement priorities for 2021, which was adopted on 5 March 2021 and released on 10 March 2021 (available in Dutch and French), collusive behaviour in response to public procurement procedures again features among the BCA's eight key sectors for enforcement (*See, this Newsletter*). Incidentally, the BCA is currently investigating high-profile allegations of bid rigging between private security firms in tendering procedures for the provision of security services to both private customers and public-sector clients such as the Belgian Ministry of Defence and NATO.

Considering the economic importance of public procurement, bid rigging in public procurement has also caught the attention of the Organisation for Economic Co-operation and Development (OECD) and the European anti-fraud office, OLAF, which have both issued extensive guidelines on the matter (available here and here).

The Notice's section on the application of the collusion-related exclusion ground provided for in the EU public procurement Directives includes a discussion on the so-called right to "self-cleaning" of tenderers (*See*, Section 5.7). The discussion considers the impact of the *RTS Infra* judgment which the Court of Justice of the European Union delivered on 14 January 2021 in response to a request for a preliminary ruling from the Belgian Council of State (*Raad van State / Conseil d'État*) (*See*, this Newsletter, Volume 2021, No. 1, p. 16).

# CORPORATE LAW

***Federal Public Service Finance Postpones Deadline for Additional Disclosure Obligations in Ultimate Beneficial Owner Register***

On 14 April 2021, the Federal Public Service Finance (the ***FPS Finance***) announced that it would postpone the deadline originally determined for submitting supporting documents demonstrating that the information in relation to the ultimate beneficial owners (***UBO***), as registered in the UBO Register, is sufficient, accurate and correct. In addition, the FPS Finance indicated that it would also postpone the deadline for making the annual confirmation of the accuracy of the information registered in the UBO Register. As a result, Belgian companies, associations and trusts now have until 31 August 2021 to comply with these obligations.

The additional disclosure obligations result from the Royal Decree of 23 September 2020 (the ***Amending Decree***) amending the Royal Decree of 30 July 2018 (the ***Decree***) regarding the functioning of 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*), which was published in the Belgian Official Journal on 1 October 2020.

In addition to various technical modifications regarding the access to, and functioning of, the UBO Register, the Amending Decree created the obligation to submit supporting documents demonstrating that the registered information is sufficient, accurate and correct (*See*, this Newsletter, Volume 2020, No. 10, p. 9).

In addition, Article 5 of the Decree provides that entities must confirm on an annual basis that the information included in the UBO Register is accurate and update this information if necessary.

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 the Decree, which specifies the information regarding the ultimate beneficial owner(s) of the specific entities that must be registered in the UBO Register (*See*, this Newsletter, Volume 2018, No. 8, p. 7).

# DATA PROTECTION

***Court of Justice of European Union Holds that Access to Traffic or Location Data in Criminal Investigation Cannot Be Authorised by Public Prosecutor***

On 2 March 2021, the Grand Chamber of the Court of Justice of the European Union (the ***CJEU***) delivered its judgment in case C-746/18, *H. K. v Prokuratuur* which deals with the access to traffic and location data in a criminal investigation under Article 15(1) of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the ***ePrivacy Directive***). The CJEU held that such access is subject to the authorisation by a fully independent authority. As a result, the access granted by the public prosecutor, who is also a party in the criminal investigation, is in breach of the ePrivacy Directive.

*Background*

In 2017, an Estonian First Instance Court found the defendant, a private individual, guilty of theft, use of another person's bank card and violence against other persons. The finding relied on personal data that was generated from the defendant's electronic communications data. The investigating authority had obtained reports containing these data from electronic telecommunications service providers in the pre-trial procedure. The access to the electronic communications data had been authorised by the Public Prosecutor's office.

The defendant appealed the decision and contested the admissibility of the reports. The defendant argued that the reports were obtained in breach of Article 15(1) of the ePrivacy Directive, read in the light of the Charter of Fundamental Rights of the European Union (the ***Charter***). The Supreme Court subsequently referred the matter to the CJEU.

*CJEU Judgment*

The CJEU first discussed its ruling in *La Quadrature du Net and Others* in which it established the conditions under which traffic and location data from electronic communications can be retained. In particular, the CJEU held that national legislation cannot impose, as a preventive measure, a general requirement on electronic communications providers to retain the general and indiscriminate traffic and location data. Only the objectives of combating serious crime or preventing serious threats to public security are capable of justifying public authorities having access to location or traffic data (*See*, this Newsletter, Volume 2020, No. 10, p. 11-13).

Second, the CJEU held that national legislation must establish the conditions under which electronic communications service providers are required to grant access to their traffic and location data to public authorities. The national legislation at issue must always apply proportionate measures, which means that the law must be clear and precise and lay down the substantive and procedural safeguards for using traffic and location data.

For these conditions to be fully observed, it is essential that a competent national authority's access to retained data is subject to prior review carried out either by an independent administrative body or a court. The CJEU specified that if such review is carried out by an independent administrative body, that entity must be impartial and free from any external influence. In particular, the administrative body cannot be involved in the conduct of the criminal investigation in question and must be neutral *vis-à-vis* the parties to the criminal proceedings. Therefore, a Public Prosecutor's office, which directs the investigation procedure and decides whether to prosecute a case, cannot authorise access to traffic and location data for the purpose of a criminal investigation. On this basis, the CJEU held that national legislation which designates the public prosecutor to act as an "independent" administrative body reviewing access to traffic and location data, is contrary to Article 15(1) of the ePrivacy Directive.

The text of the CJEU judgment can be found here.

***Belgian Data Protection Authority Fines Telecommunications Provider for Inadequate Security Measures to Prevent Data Breach in Context of "SIM Swapping"***

On 22 January 2021, 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 25,000 on a telecommunications provider for failing to put in place adequate security measures against data breaches as required by General Data Protection Regulation (EU) 2016/679 (the ***GDPR***).

*Factual Background*

In September 2019, a customer (the ***Complainant***) lodged a complaint with the Litigation Chamber claiming that his telecommunications provider (the ***Telecommunications Provider***) had failed to implement adequate security measures to prevent a personal data breach. The Complainant had been a customer of the Telecommunications Provider since 2015, using prepaid telephone services. In 2019, a third party visited one of the Telecommunications Provider's stores, presenting the phone number and SIM card number of the Complainant. The third party requested that the prepaid subscription of the Complainant should be converted into a post-paid subscription.

It is unclear how the third party was able to access the Complainant's data, and for which purposes the third party intended to use the Complainant's phone number. The third party gave the Telecommunications Provider his own identity data, linking it to the post-paid subscription so that all charges would be billed in the third party's name. According to the Litigation Chamber, this made it less likely that the scheme was intended to be used for identity theft or fraud, since it would be easy to identify the third party responsible for the scheme.

Four days after converting the Complainant's subscription, the third party requested a new SIM card connected to that same mobile number. Through this SIM card, the third party gained access to the mobile number of the Complainant and the SIM card of the Complainant was deactivated. Only after four days, and several calls and visits to the Telecommunications Provider, the Complainant recovered his phone number.

The Telecommunications Provider argued that for several reasons it could not be held liable for the data breach. First, only the user of a mobile phone number would know the associated SIM card number. Second, it had been unable to carry out an identity check of the individual requesting the change, as this would be prohibited under the Law on Electronic Communications of 15 June 2005 (*Wet betreffende de elektronische communicatie / Loi relative aux communications électroniques*). Third, the infringement had had very limited consequences for the Complainant. As a result, the Telecommunications Provider had not considered it necessary to notify the DPA and the Complainant of the data breach under the GDPR.

*Decision*

The DPA rejected the position of the Telecommunications Provider and held that the latter had taken insufficient measures to prevent a personal data breach. According to the DPA, the Law on Electronic Communications cannot be interpreted as preventing an identity verification, when this verification is carried out to prevent a customer's mobile number from being wrongfully appropriated by a third party who thereby secured access to the original owner's mobile telephone traffic and potentially to services linked to the mobile number, such as PayPal and WhatsApp.

The DPA also rejected the argument that the infringement had had limited consequences for the Complainant. It pointed out that in its *Digital Rights Ireland* ruling of 8 April 2014, the Court of Justice of the European Union held that telecommunications data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained. This includes information on daily life habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. The DPA added that there was a considerable chance that the third party could have obtained access to personal data of the Complainant, such as texts about medical appointments and conversations and messages. On this basis, the DPA concluded that the privacy rights of the Complainant had been significantly at risk because of the data breach.

The DPA thus held that by not carrying out an identity verification of the third party, the Telecommunications Provider had failed its obligations under the GDPR, which require it to ensure appropriate security of its data processing activities. Furthermore, the Telecommunications Provider had also infringed the GDPR by failing to notify the data breach to the DPA and to the Complainant. The DPA imposed a fine of EUR 25,000.

The DPA decision is available in Dutch.

***Belgian Data Protection Authority Prohibits Use of Unlawfully Obtained Personal Data in Arbitration Proceedings***

In a decision of 29 January 2021, the Litigation Chamber (*Geschillenkamer / Chambre contentieuse*) of the Belgian Data Protection Authority (*Gegevensbeschermingsautoriteit / Autorité de protection des données* - the ***DPA***) prohibited a controller from passing on personal data obtained in breach of data protection rules to its legal counsel. The Litigation Chamber did not issue a fine, but the decision serves as a clear message that further processing of unlawfully obtained personal data, even in the context of legal proceedings, is prohibited.

The dispute before the DPA involved an individual practising as a notary public (the ***Plaintiff***), her accountant (the ***First Defendant***) and her former business partner who is also practising as a notary (the ***Second Defendant***). The case at hand arose in arbitration proceedings relating to the winding-up of the practice of a notary public due to financial issues and the refusal to submit specific accounting documents and other information.

The First Defendant mistakenly forwarded an e-mail with 32 annexes, which contained personal data relating to the Plaintiff, to the Second Defendant. This resulted in the disclosure of data relating to the Plaintiff's personal activities, finances, and other personal data to the Second Defendant, without the Plaintiff's consent. In turn, the Second Defendant forwarded the e-mail and its annexes to his legal counsel, who then used the e-mail and its annexes as an exhibit in the arbitration proceedings between the Second Defendant and the Plaintiff.

*Processing by First Defendant*

In the proceedings before the Litigation Chamber, the First Defendant argued that the communication of the e-mail and its annexes to the Second Defendant resulted from his habit of sending e-mails to both the Plaintiff and the Second Defendant. As this transfer was unintentional, the First Defendant argued that it could not constitute a violation of General Data Protection Regulation (EU) 2016/679 (the ***GDPR***). However, the Litigation Chamber noted that the transfer of personal data constituted a form of processing within the meaning of the GDPR and that the intent was irrelevant.

The Litigation Chamber went on to assess whether the processing could be justified by the pursuit of a legitimate interest of the First Defendant. Pursuant to Article 6(1)(f) of the GDPR, personal data may be processed if this is necessary for the legitimate interests pursued by the controller, the third party or parties to whom the data are disclosed, and as long as such interests are not overridden by the interests or fundamental rights of the data subject. The Litigation Chamber found that, although the processing was carried out in the pursuit of a legitimate interest of the First Defendant, the latter could have sent an e-mail to both the Plaintiff and the Second Defendant concerning the notary practice and a separate e-mail to the Plaintiff only concerning her personal company. As a result, the First Defendant did not apply the data minimisation principle. Additionally, the Litigation Chamber found that the Plaintiff had resorted to the First Defendant's services for the preparation and maintenance of the accounting documents relating to her personal company and could not have expected the First Defendant to share data processed in this context to the Second Defendant.

On this basis, the Litigation Chamber concluded that the transfer of the e-mail and its annexes by the First Defendant to the Second Defendant could not be justified by the legitimate interests of the First Defendant and did not have any other distinct legal basis under Article 6 of the GDPR. Accordingly, it found that the First Defendant had infringed Articles 5(1)(a) in combination with 6(1), 5(1)(b) in combination with 6(4), and 5(1)(c) of the GDPR. However, the First Defendant demonstrated that he immediately took steps to have the Second Defendant delete the e-mail and to inform the Plaintiff's counsel of such deletion. This was also the First Defendant's first infringement of the GDPR. As a result, the Litigation Chamber decided not to impose an administrative fine, but instead only to reprimand the First Defendant.

*Processing by Second Defendant and Legal Counsel*

The Second Defendant argued that he had simply been a recipient of the e-mail and its annexes and, as such, could not be considered to have processed the Plaintiff's personal data. However, before deleting the e-mail and its annexes as requested by the First Defendant, the Second Defendant had transferred the e-mail and its annexes to his legal counsel. The Litigation Chamber observed that the consultation of the annexes and the transfer of the e-mail and its annexes to his legal counsel amounted to a form of processing within the meaning of the GDPR. The Litigation Chamber also noted that the Second Defendant did not show that his legal counsel had also deleted the e-mail and its annexes.

The Second Defendant then attempted to justify the transfer of the e-mail and its annexes to his legal counsel by the privileged and confidential character of attorney-client correspondence. The Litigation Chamber did not accept this argument, stating that, although clients must be able to make confidential communications to their lawyers, such communications must still comply with the GDPR if they contain a third party's personal data. Accordingly, a client cannot communicate unlawfully obtained personal data to a legal counsel and justify its further processing for use in pending or future legal proceedings, without violating the principles of lawfulness, loyalty and transparency.

The Litigation Chamber concluded that the processing of the e-mail and its annexes by the Second Defendant had infringed Articles 5(1)(a) and 6(1) of the GDPR. Here also, as this was the Second Defendant's first infringement of the GDPR, the Litigation Chamber decided not to impose an administrative fine. However, it prohibited the processing of the illegally obtained personal data and ordered the Second Defendant to inform its legal counsel that the use of the relevant personal data was prohibited.

The DPA's decision can be appealed to the Markets Court (*Marktenhof / Cour des marchés*). The decision is available in Dutch (here).

***European Data Protection Board Clarifies Application of General Data Protection Regulation to Processing for Health-Related Research***

On 2 February 2021, the European Data Protection Board (***EDPB***) replied to several questions for clarification from the European Commission on the consistent application of the General Data Protection Regulation (EU) 2016/679 (***GDPR***) to data processing for health-related research (the ***EDPB Response***). In that response, the EDPB addresses some misunderstandings on the application of the GDPR in scientific health research activities. However, the EDPB Response does not address all the European Commission's questions. It indicates that the outstanding questions will be addressed in detail in the EDPB's upcoming "Guidelines on the processing of personal data for scientific research purposes". These guidelines are currently under preparation and will be published in the course of 2021.

The main questions addressed by the EDPB Response are summarised below.

*Establishing Legal Grounds for Processing for Health-related Research*

First, the EDPB clarifies that ethics standards (such as the Declaration of Helsinki) do not imply that only explicit consent can be used to legitimise the processing of health data for scientific research purposes. Other legal grounds foreseen in Article 6 of the GDPR can still be used for such processing purposes. Importantly, the EDPB points out that, where controllers process health data for scientific research purposes, they also must satisfy one of the exemptions of Article 9(2) of the GDPR that can be relied upon for processing health data.

However, regardless of the legal ground on which the processing is based under the GDPR (i.e., whether that is consent or not), an informed consent to participate in the medical research project is required. In other words, the legal basis for the processing of personal data comes on top of the consent that is required under separate ethical (and legal) rules. This is because ethical rules and bio-ethics conventions protect individuals against being included in medical research projects against their will and/or without their knowledge.

A further complication is that the specific purpose of scientific research may be difficult to determine at the outset. If the purposes for processing within a scientific research project cannot be specified at the outset, recital 33 of the GDPR allows, by way of exception, that the purpose may be described at a more general level. In that case, the controller must find other ways for ensuring that the essence of the consent requirements is best served, for example, by allowing data subjects to consent to specific stages of the research that are already known to take place at the outset.

*Medical Research Participants with Power Imbalance*

The EDPB points out that consent is not an appropriate legal basis in research activities if there is a clear imbalance of power between the data subject and the controller. Depending on the circumstances, such an imbalance may exist in clinical trials, for instance, when the data subject is not in a good health and there is no other therapeutic treatment available, in addition to the treatment offered by the clinical trial. A particularly thorough assessment of trial circumstances must be carried out to determine if consent is appropriate.

*Medical Research in Multiple Member States*

The EDPB recommends using, whenever possible, the same legal processing basis if a health research project is conducted in multiple Member States. However, the use of a heterogeneous legal basis cannot be excluded due to the considerable differences in Member State laws. The EDPB advises controllers to limit the consequences of different legal regimes as much as possible, for instance by optimising and harmonising the rights of data subjects, irrespective of the Member State they live in.

*Further Processing*

The EDPB will clarify the requirement of a legal basis for "further processing" for scientific research purposes (by the original or a subsequent controller) in the guidelines which it is currently preparing. However, it already indicates that for the presumption of compatible use of Article 5(1)(b) of the GDPR to apply (*i.e.*, compatible use for further processing of health data for scientific research purposes), adequate safeguards as required by Article 89(1) of the GDPR must be put in place (such safeguards may include pseudonymisation but the EDPB will elaborate on these "adequate safeguards" in its guidelines).

In addition, Article 9 of the GDPR may come into play if the exemption from the prohibition on the processing of health data which the health care provider relied on for the original purpose does not extend to the processing of health data for scientific research purposes. For instance, if the exemption in Member State law only allows for the processing of health data by the health care provider to provide medical treatments (Article 9(2)(h) of the GDPR), the health care provider would still have to rely on an exemption based on Union or Member State law as required by Article 9(2) of the GDPR for the processing of health data for scientific research purposes.

*Pseudonymisation and Anonymisation*

The EDPB indicates that pseudonymisation constitutes an additional safeguard that should be employed for scientific research to ensure respect for the principle of data minimisation in accordance with Article 89(1) of the GDPR. Anonymisation is a distinguished concept since anonymised data are considered not to fall under the scope of the GDPR while pseudonymised data do. The EDPB notes that anonymisation should be approached with caution in the context of scientific research because anonymisation of personal data can be difficult to achieve (and maintain). Ongoing advancements in available technology and re identification techniques make anonymisation increasingly complex.

With regard to genetic data, the EDPB questions whether any combination of technical and organisational means can be effectively employed to remove genetic information from the material scope of the GDPR. In any case, in the interests of protecting the rights and freedoms of individual data subjects, the EDPB strongly advises that genetic data be treated as personal data and that its processing be conducted on the basis of appropriate technical and organisational measures to ensure compliance with the GDPR.

The EDPB Response can be consulted here.

***European Data Protection Board Publishes 2021-2022 Work Programme***

On 16 March 2021, the European Data Protection Board (***EDPB***) published its 2021-2022 work programme (the ***Work Programme***). This follows the adoption of the EDPB's 2021-2023 strategy in December 2020 (*See*, this Newsletter, Volume 2020, No. 12, p. 9) and is centred on four main pillars set out below.

*Enhancing Harmonisation and Facilitating Compliance*

In addition to providing practical and accessible guidance, the EDPB will develop and promote tools that help implementing data protection in practice. Additionally, efforts will be made to use the consistency mechanism and other tools to address potential divergences in applying General Data Protection Regulation (EU) 2016/679 (the ***GDPR***). As a result, there will be further guidance on key notions of EU data protection law such as data subject rights, protection of children's data and processing for medical and scientific research purposes.

*Supporting Effective Enforcement and Efficient Cooperation between National Supervisory Authorities*

The EDPB will facilitate a more efficient functioning of the cooperation and consistency mechanism by streamlining internal processes, combining expertise and promoting enhanced coordination between national supervisory authorities. It will also seek to develop a genuine EU-wide enforcement culture among supervisory authorities. The envisaged work under this pillar covers guidance on the one-stop-shop mechanism and the calculation of administrative fines.

*Preserving Fundamental Rights in Face of New Technologies*

Under this pillar, the EDPB will monitor new and emerging technologies and their likely impact on the fundamental rights and daily lives of individuals. The EDPB will also help shape Europe's digital future while continuing to work with other regulators and policymakers to promote regulatory coherence and enhanced protection for individuals. The focus will be on establishing guidelines on blockchain, anonymisation and pseudonymisation. Furthermore, the EDPB will look at the use of facial recognition in the area of law enforcement, social media platform interfaces and other technological issues such as cloud computing, the internet of things and data brokers.

*Global Dimension of Data Protection*

In considering the global dimension, the EDPB's goal is to set and promote high EU and global standards for international data transfers to third countries. The EDPB will focus on opinions on and the review of adequacy decisions, guidelines on codes of conduct and certifications as tools for international transfers and the territorial scope of the GDPR.

The EDPB's 2021-2022 Work Programme can be found here.

***Joint Opinion of European Data Protection Board and European Data Protection Supervisor on Data Governance Act***

On 11 March 2021, the European Data Protection Board (***EDPB***) and the European Data Protection Supervisor (***EDPS***) published their joint opinion on the European Commission's proposed Regulation on data governance (the ***Data Governance Act*** or ***DGA***; *See*, this Newsletter, Volume 2020, No. 11, p. 10). The proposed DGA is the first of a set of measures announced in the European Data Strategy unveiled by the Commission in March 2020 (*See* our Note on the European Data Strategy here).

The EDPB and EDPS recognise the essential role which the DGA plays for the proposed data-driven economy framework. They further acknowledge the legitimate objective of increasing the availability of data for use by enhancing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU. However, the joint opinion also notes the failure of the DGA to consider the fundamental right to personal data protection and notes that the DGA is not sufficiently in line with existing EU law.

The joint opinion raises several concerns and possible conflicts of the proposed DGA with General Data Protection Regulation 2016/679 (the ***GDPR***). These include (i) the legal basis for the processing of personal data; (ii) an unclear distinction between the processing of personal and non-per-

sonal data and an unclear relationship between the DGA and Regulation 2018/1807 on free flows of non-personal data; and (iii) an inconsistent use of definitions and key concepts that are also used in the GDPR.

As regards the subject matter and scope of the DGA, the EDPB and EDPS recommend introducing a provision which unambiguously states that the DGA will leave intact the level of protection of individuals with regard to the processing of personal data under the provisions of Union and national law. Additionally, the DGA cannot alter any obligations and rights set out in the data protection legislation. More generally, any proposal, including upcoming initiatives related to data that may have an impact on the processing of personal data, must ensure the continued application of personal data protection rules.

Furthermore, according to the EDPB and EDPS, the DGA should define the different roles relevant from the perspective of personal data protection law (*e.g.*, data controller, processor, or joint controller). Concepts such as "data sharing service provider", "data altruism organisation", and "data user" will also have to be defined.

Finally, the joint opinion is of the opinion that the governance and monitoring of compliance provided for by the proposed DGA should be strengthened.

The joint opinion can be consulted here.

***Belgian Data Protection Authority Publishes New Tools and Templates***

On 16 March 2021, the Belgian Data Protection Authority (*Gegevensbeschermingsautoriteit / Autorité de protection des données* - the ***DPA***) published new tools, templates and other documents for use by controllers, processors and Data Protection Officers (***DPOs***). The documents are available in Dutch and in French.

The documents published include a simplified model for registering processing activities, a roadmap on exchanges of personal data by/with federal governmental authorities and a template protocol for the communication of personal data between governmental authorities in accordance with Article 20 of the Law of 30 July 2018 on the protection of individuals with regard to the processing of personal data.

For small and medium enterprises (***SMEs***), the new documents include FAQs and templates for dealing with data subjects' rights.

# INSOLVENCY

***Law Providing for Pre-packaged Insolvency Procedure and Enhanced Accessibility to Judicial Reorganisation Procedure Enters into Force***

On 26 March 2021, the Law modifying Book XX of the Code of Economic Law entered into force, subject to exceptions (*Wet tot wijziging van Boek XX van het Wetboek van Economisch Recht en het Wetboek van de Inkomstenbelastingen 1992 / Loi modifiant le livre XX du Code de droit économique et le Code des impôts sur les revenus 1992* - the ***Law***).

In response to the Covid-19 crisis, the federal government granted two temporary moratoria during which Belgian businesses were generally protected against (i) bankruptcy and judicial dissolution; (ii) attachment and enforcement measures; and (iii) termination of existing contracts because of a failure to pay. Following the termination of the second moratorium on 31 January 2021, the federal government promised reforms to the insolvency code to help economically viable companies in their recovery from the Covid-19 crisis (*See*, this Newsletter, Volume 2021, No. 1). While working out these reforms, the federal government ordered the tax and social security authorities not to bring any actions for bankruptcy against businesses that have outstanding tax or social security debts.

The Law principally (i) introduces a pre-packaged insolvency procedure; and (ii) makes the judicial reorganisation procedure more accessible.

*Pre-Packaged Insolvency Procedure*

Inspired by the "pre-packs" used in insolvency filings in the U.S., the Law introduces a legislative framework that allows companies in financial difficulties to prepare an out-of-court restructuring plan with their main creditors prior to submitting an official request for judicial reorganisation in court. The procedure allows for a fast-track reorganisation plan to be negotiated without the negative consequences associated with the publicity and burdensome procedure of a conventional judicial reorganisation procedure.

As a general principle, a creditor's enforcement rights are not suspended while negotiating an agreement with the company in the "pre-pack stage". However, the court can impose specific conditions on the payment of debt to creditors. The court also has the power to suspend the creditors' enforcement rights temporarily. The duration of these restrictions must not exceed four months.

A court-appointed judicial officer must assist the company in the negotiations with its creditors and in working out the terms of a restructuring plan. If the negotiations are successful, the "pre-packaged" restructuring plan should allow the company to run through the formal judicial reorganisation procedure quickly, receive the authorisation of the court, and complete its reorganisation.

*Enhanced Accessibility to Judicial Reorganisation Procedure*

The Law also abolishes specific burdensome disclosure obligations to the court before a company can qualify for protection from its creditors under a judicial reorganisation procedure. The requisite information can now be supplied at a later stage or may even be waived.

Most provisions of the Law only apply until 30 June 2021, but this expiry date is subject to an extension determined by Royal Decree.

***Labour Court of Appeal of Antwerp Convicts Belgian State for Failing to Implement Correctly EU Directive Offering Protection to Employees in Judicial Reorganisation***

*See*, this Newsletter, current issue, section on Labour Law.

# INTELLECTUAL PROPERTY

***Court of Justice of European Union Prohibits Circumventing Restrictions on Linking to Copyright Protected Content***

On 9 March 2021, the Court of Justice of the European Union (***CJEU***) confirmed in case C-392/19 *VG Bild-Kunst* that a right holder is allowed to adopt technical measures to restrict links to protected content. The CJEU held that Article 3(1) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (***InfoSoc Directive***) must be interpreted to mean that embedding by means of framing in a third-party website page constitutes a communication to the public. As a result, any links that circumvent the original restrictions on embedding are subject to authorisation by the right holder.

*Factual Background and Procedure*

The request for a preliminary ruling was made by the *Bundesgerichtshof* (German Federal Court of Justice) in a dispute involving VG Bild-Kunst, a copyright collecting society, and SPK, an operator of the Deutsche Digitale Bibliothek (DDB), a digital library devoted to culture. The DDB website stored thumbnails of original images with the authorisation of the copyright holders. VG Bild-Kunst required SPK to implement effective technological measures against the framing by third parties of the protected works' thumbnails in the digital library. However, SPK refused and considered that such a measure would be unreasonable and in violation of copyright legislation. SPK brought an action before the Regional Court in Berlin seeking a declaration that VG Bild-Kunst was required to offer a licence. However, the Berlin court dismissed SPK's claim. On appeal, the Higher Regional Court of Berlin set aside the first judgment. VG Bild-Kunst appealed this decision to the *Bundesgerichtshof* which in turn called on the CJEU for a preliminary ruling.

*Advocate General's Opinion*

On 10 September 2020, Advocate General (***AG***) Szpunar handed down his opinion, proposing to make a distinction between automatic and clickable links. The AG explained that for automatic links, the right holder's consent is required as the embedding of the protected content is automatically displayed on the provider's website and thus targets a "new public". In such a case, the user can see the protected work without being redirected to a new page. By contrast, for clickable links, the user is redirected when accessing the protected work. The AG was of the opinion that the right holder's consent is not required in that case since the link does not target a new public.

*CJEU Judgment*

The CJEU did not follow the AG's opinion, and focused on the position of the right holder, rather than the nature of the link. The CJEU distinguished between two scenarios: in the first one, the right holder communicates the work without technological measures to restrict its access and is then considered to authorise access to all internet users. In the second one, the right hold uses restrictive measures to limit access to the protected work. Under that approach, the CJEU considered that the right holder cannot be deemed to have authorised access to all internet users. As a consequence, a linking method that circumvents these measures requires the right holder's consent.

The CJEU's judgment can be found here.

***AG Szpunar Gives Opinion on Decompiling Computer Programmes***

On 10 March 2021, Advocate General (***AG***) Szpunar delivered his opinion in case C-13/20 *Top System SA v. Belgian State*. The AG suggested that Article 5(1) of Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programmes (the ***Software Directive***) allows the lawful acquirer of the software to decompile a computer programme to correct errors in the software.

*Factual Background and Procedure*

The dispute arose between Selor, the selection and recruitment office of the Belgian federal government, and Top

System, a software company. Selor had decompiled Top System's software to address a malfunction. The decompiling of a programme is a process of reverse engineering involving the conversion of an executable programme code into a readable form. Top System objected to the decompiling and brought an action for copyright infringement which ended up before the Court of Appeal of Brussels (*Hof van Beroep te Brussel / Cour d'appel de Bruxelles*). That court referred a request for a preliminary ruling to the Court of Justice of the European Union.

*Advocate General's Opinion*

The AG observed that even if decompiling is not mentioned in Article 4 of the Software Directive, which provides for the exclusive rights of the author of the programme, a combination of acts required for decompiling, such as reproduction and alteration, are within the author's monopoly. On the other hand, Article 5 of the Software Directive indicates that in the absence of contractual provisions, the acquirer can carry out acts that are within the owner's monopoly provided these are necessary for the use of the programme, including correcting its errors.

The AG noted that Article 5 of the Software Directive lists the acts that are necessary for the programme's use and Article 6 of the Software Directive allows decompiling software by an authorised user (without the author's authorisation) when this is indispensable for the interoperability of the software and when the information necessary for ensuring interoperability is not readily available. The AG did not follow Top System's position that Article 6 should prevail over Article 5, and therefore decompiling can only be performed for interoperability purposes and never to correct software errors. Instead, the AG suggested that Article 5 be interpreted as allowing the lawful acquirer to decompile the software when it is necessary to correct errors affecting its proper functioning.

The AG added that the only justification to decompile a programme is to correct an error that prevents its proper functioning. The programme's function is defined by the author or, in some cases, is the result of the agreement between the supplier and the buyer of the programme. Article 5 of the Software Directive should thus be interpreted as meaning that the decompiling of a computer programme carried out by the lawful acquirer to correct errors in the software is not subject to the conditions of Article 6 of the Software Directive. However, the decompiling can only be carried out for correction purposes and within the acquirer's contractual limits.

The AG's opinion can be found here.

# LABOUR LAW

***Criminal Court Penalises Employer for Not Adopting Adequate Work Floor Measures to Prevent Burnout***

On 24 February 2021, the French-language Criminal Court of Brussels (the ***Criminal Court***) imposed a criminal fine involving community service on an employer for not adopting adequate measures to prevent burnout of his employees and, more generally, psychosocial risks at work.

The obligation for employers to adopt preventive measures to avoid burnout and other psychosocial risks at work is provided for by the Law of 4 August 1996 on the well-being of employees during the performance of their work (*Wet betreffende het welzijn van de werknemers bij de uitvoering van hun werk / Loi relative au bien-être des travailleurs lors de l'exécution de leur travail* - the ***Law on Well-Being***).

*Factual Background*

Psychosocial risks at work are defined as the likelihood that one or more employees will suffer psychological damage, which may or may not involve physical harm, because of exposure to the elements of the work organisation, job content, working conditions, working circumstances and interpersonal relationships at work, on which the employer has an impact, and which objectively entail a danger.

In the case at hand, several employees were suffering from psychosocial trauma and/or a burnout which was caused by a stressful and a disrespectful working environment.

The Criminal Court considered the following facts to be relevant:

- one employee representative, a trade union delegate, filed a complaint for psychological harassment with the external service for prevention and protection at work (the ***External Service***) challenging the psychologically violent behaviour of the operational director of the employer and its impact on her health status. The other employee representatives confirmed this behaviour and requested further action from the employer. However, the employer failed to adopt any specific measures to prevent future unacceptable behaviour from the operational director. The employee representative concerned was diagnosed with burnout due to the stressful working environment and committed suicide in 2018;

- several other employees filed complaints for psychosocial intervention with the External Service, referring to an excessive and unacceptable workload, harassment, burnout, racist remarks, invasion of privacy and intimidation at work;

- the External Service and the Interfederal Centre for Equal Opportunities (*Interfederaal Gelijkekansencentrum/Centre Interfédéral pour l'égalité des chances*) issued multiple warnings and/or formal reports which addressed issues in relation to discrimination and the lack of preventive measures to cope with psychosocial risks at work; and

- the employee representatives within the Committee for Prevention and Protection at work requested a profound psychosocial risk analysis to be undertaken by the employer with the assistance of the appropriate stakeholders.

*Criminal Court Analysis*

The labour prosecutor pressed charges against the employer and two directors, who qualified as the employer's delegates, before the Criminal Court which found the employer to be in breach of the Law on Well-Being for:

- failing to adopt individual and/or collective measures to prevent or limit psychosocial risks at work and in particular burnout; and

- not taking appropriate action towards the operational director following several complaints emphasising his intimidating and psychologically violent behaviour.

The Criminal Court stressed the employer's passive approach in relation to the prevention of psychosocial risks at work considering the numerous complaints of the employees. Hence, it convicted the employer to pay the maximum criminal fine of EUR 8,000. However, payment was partially suspended, given the employer's lack of criminal record and its community service.

By contrast, the Criminal Court acquitted the directors in view of the general criminal law principle applicable at the time of the facts which precluded the employer and the private individuals from being found guilty of the same infringements. The Criminal Court had to determine which party committed the most serious fault and could only convict that party. The Criminal Court considered that the directors had only followed the clear instructions regarding the workload of the employees that were given by the municipal political powers which subsidised the employer. On that basis, the Criminal Court only convicted the employer.

***Labour Court of Appeal of Antwerp Convicts Belgian State for Failing to Implement Correctly EU Directive Offering Protection to Employees in Judicial Reorganisation***

*Background*

In case C-55/18, *CCOO v. Deutsche Bank* (*See*, this Newsletter, Volume 2019, No. 5, p. 15), the Court of Justice of the European Union (***CJEU***) applied Directive 2001/23/EC on the approximation of the laws of the Member States relating to the safeguarding of employees' rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses (the ***Directive***). The CJEU held that the Directive prohibits national legislation which entitles the transferee of a business in a judicial reorganisation under judicial authority to choose the employees whom it wishes to keep without offering any proof of the reasons for dismissing the employees who are not retained.

As a consequence, current Article XX.86 §3 of the Belgian Code of Economic Law (the ***CEL***) is not in line with the Directive, as it does not impose a requirement on the transferee to justify its choice of the employees that are made redundant, and to prove the economic, technical or organisational reasons of such redundancies in a judicial reorganisation by transfer under judicial authority.

*Judgment*

Following the preliminary ruling of the CJEU, the case was referred back to the Labour Court of Appeal of Antwerp (the ***Labour Court of Appeal***) which had initially stayed the proceedings in order to obtain the CJEU's judgment.

On that basis, the plaintiff, Ms. Plessers, decided to seek damages from the Belgian State for its failure to implement the Directive correctly in Belgian law. Ms. Plessers considered her injury to amount to the severance pay which she should have been granted by the transferee following its decision not to maintain her employment. She argued that, if the Directive had been implemented correctly, the transferee would have been obliged to take over all the employees, including herself. Failing her transfer, the transferee would have terminated her employment agreement unlawfully and she would have been entitled to severance pay.

In its judgment of 24 March 2021, the Labour Court of Appeal confirmed that Belgian law is not in line with the Directive. However, it pointed out that Belgium could have adopted alternative legislation, consistent with the Directive, based on which the transferee should have demonstrated prior to any transfer that any decision not to keep a specific employee after the transfer but to dismiss him or her, is justified for economic, technical or organisational reasons that are not linked to the transfer itself and entail changes in the workforce. The Labour Court of Appeal stressed that the preliminary ruling of the CJEU explicitly indicated that the Directive does not prevent such dismissals.

On this basis, the Labour Court of Appeal considered that there was no causal link between the Belgian State's fault, *i.e.*, not transposing the Directive correctly into Belgian law, and the alleged injury of the plaintiff, *i.e.*, the loss of employment. The Labour Court of Appeal therefore rejected Ms. Plessers' action for damages amounting to severance pay.

Despite this, the Labour Court of Appeal still granted Ms. Plessers token damages for a loss of a potential chance of employment. The Labour Court of Appeal pointed out that the transferee had actually invoked detailed economic, technical and organisational reasons showing why Ms.

Plessers had not been retained. It added that these reasons had not even been disputed by Ms. Plessers. Hence, it considered it unlikely that the Enterprise Court which had to decide on the transfer would not have accepted these reasons for dismissal. As a result, it evaluated the damages due to Ms. Plessers at EUR 1,000 only.

*Legislative Development*

In the meantime, and further to the preliminary ruling of the CJEU, a private members' bill was submitted on 21 October 2020 to amend Book XX of the CEL to bring it in line with the Directive (bill 55K1591). The proposal seeks to modify Articles XX.39 and XX.86 of the CEL to introduce an obligation for the transferee to justify the decision to take over only specific employees and dismiss others for economic, technical or organisational reasons. This procedure will be supervised by the Enterprise Court which is also in charge of the judicial reorganisation procedure.

The proposal is still pending, and it is possible that the envisaged amendments will be considered together with the amendments required to implement Directive 2019/1023 on preventive restructuring frameworks, on discharge of debt and disqualifications, and on measures to increase the efficiency of procedures concerning restructuring, insolvency and discharge of debt, and amending Directive (EU) 2017/1132 into Belgian law (which must be implemented by 17 July 2021).

# PUBLIC PROCUREMENT

***European Commission Issues Notice on Tools to Fight Collusion in Public Procurement***

*See*, this Newsletter, section on Competition Law.

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