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

Legal 500 2019

June 2021

VBB on Belgian Business Law

Highlights

CAPITAL MARKETS AND FINANCIAL LAW
Financial Services and Markets Authority Establishes Minimum Standards for Special Purpose Acquisition Companies
Page 3

COMPETITION LAW
Belgian Competition Authority Clears Acquisition of Mobile Vikings by Proximus
Page 7

DATA PROTECTION
In Belgian Case Involving Facebook Court of Justice of European Union Clarifies When Supervisory Authorities Can Derogate from One-Stop-Shop Principle
Page 9

INSOLVENCY
Term of Pre-packaged Insolvency Procedure and Enhanced Accessibility to Judicial Reorganisation Procedure Extended
Page 16

INTELLECTUAL PROPERTY
At Request of Antwerp Enterprise Court, Court of Justice of European Union Analyses Communications to Public for Copyright Purposes and Recognises Right To Sue of Non-Practising Entities
Page 17

LITIGATION
Brussels Court of First Instance Finds Against Belgian Federal and Regional Governments in Climate Litigation
Page 20

"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

CAPITAL MARKETS AND FINANCIAL LAW

Financial Services and Markets Authority Establishes Minimum Standards for Special Purpose Acquisition Companies

On 21 June 2021, the Financial Services and Markets Authority (***FSMA***) published a position paper proposing minimum standards for the structuring of special purpose acquisition companies (***SPACs***). The paper also discusses the disclosing of information regarding SPACs and their trading on Euronext Brussels. The minimum standards envisaged by the paper seek to protect investors against making uninformed decisions when investing in a SPAC. This is because SPACs are considered to be complex investment products subject to specific valuation methods. For example, investors should be conscious of the risks of conflicts of interest and of dilution of their participation in a SPAC.

The FSMA encourages issuers of shares in a SPAC to offer maximum protection and transparency to potential investors.

Concept of SPACs

A SPAC, also referred to as a 'blank check company', is a company with no operating history that raises capital through an initial public offering (***IPO***). Subsequently, with the funds collected through the IPO, the SPAC acquires, and then merges with, a non-listed business. This business combination is typically carried out within a short timeframe of up to 24 months following the IPO. This allows the acquired business to go public while avoiding the extensive disclosures which it would normally have to deal with during the IPO process. SPAC transactions have seen a meteoric rise in the United States in 2020 and 2021, and, although still less frequently used in Europe, are now also surging in Europe. Until now, no SPAC has been listed on Euronext Brussels.

Governance and Conflicts of Interest

The first set of minimum standards put forward by the FSMA relates to the governance of a SPAC. These standards intend to offer investors maximum protection against the risk of potential conflicts of interest. For example, the FSMA proposes that the business combination should be approved by the shareholders of the SPAC (who will suffer the impact of a dilution resulting from that business combination) instead of its directors.

In addition, the FSMA recommends introducing a strict dealing code pursuant to which the founders and/or sponsors of the SPAC would be prohibited from trading any securities during the negotiation phase of the business combination.

Exit Arrangements

A key feature of the IPO of the SPAC is that the shares sold to the public are redeemable. The SPAC is required to offer the public shareholders the right to redeem their shares upon approval of the business combination if they do not wish to remain shareholders of the merged entity.

The FSMA proposes to limit such redemption right to shareholders who voted against the business combination (which is likely to result in dilution of the shareholders in the SPAC) as any redemption of shares leads to an additional dilution of the shares held by the remaining shareholders.

Setting out Scenarios of Dilution in Prospectus

The SPAC is required to publish a prospectus as part of its IPO. According to the FSMA, this prospectus must contain a simulation of different dilution scenarios and an estimate of the required annual rate of return for the shareholders to neutralise the impact of such dilution.

To catch the attention of potential investors, a reference to the section of the prospectus covering the dilution scenarios must be included on the cover page of the prospectus.

Limitation of Ownership of SPAC Shares to Professional Investors

The FSMA further proposes to limit the trading in SPAC shares on Euronext Brussels to professional investors only. Retail investors would be able to sell or buy SPAC shares (i) through a financial institution (in which case the financial institution should assess whether the retail investor has sufficient knowledge and experience in relation to this kind of investment) or (ii) directly by meeting a suitability test.

Transparency on Minimum Standards

The position paper of the FSMA concludes that founders and/or sponsors who do not wish to comply with the above minimum standards should explicitly disclose this on the cover page of the prospectus by using the FSMA's template wording.

The minimum standards introduced by the FSMA can be consulted here.

COMMERCIAL LAW

Supreme Court Requests Court of Justice of European Union to Shed Light on Validity of General Terms and Conditions Referred to by Hyperlink

On 20 May 2021, the Supreme Court (*Hof van Cassatie / Cour de Cassation*) considered the validity and enforceability of a forum selection clause contained in general terms and conditions (***GTCs***) referred to by way of a hyperlink in a contract. Deciding to stay the proceedings, the Supreme Court referred this issue to the Court of Justice of the European Union (***CJEU***) for a preliminary ruling. As GTCs are ubiquitous in commercial interactions and typically contain forum selection clauses, the CJEU's judgment is expected to provide much-anticipated clarifications.

Background

The dispute at hand pits the Belgian company Tilman SA (***Tilman***) against the Swiss company Unilever Supply Chain Company AG (***Unilever***) (together, the ***Parties***). In 2011, the Parties signed a service agreement under the terms of which Tilman would package tea bags in boxes against a given price and would invoice materials to Unilever on a separate basis. A dispute arose regarding the amounts due to Tilman in accordance with the service contract, and Tilman initiated proceedings against Unilever for the payment of outstanding sums before a commercial court (now: enterprise court).

Importantly, the service agreement specified that the Parties' obligations were to be performed in accordance with Unilever's general terms and conditions (***GTCs***), which were referred to by way of a hyperlink. In turn, Unilever's GTCs provided for the exclusive jurisdiction of English courts and expressly excluded the application to the contract of the supplier's GTCs. Additionally, Unilever's GTCs provided for the applicability of the 2007 Lugano Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (the ***Lugano II Convention***).

In 2015, the commercial court determined in first instance that Belgian courts had jurisdiction over the dispute at hand, but that the service agreement was governed by English law. Both Parties appealed the first-instance judgment: Tilman because the court had declined to apply Belgian law, and Unilever insofar as the judgment ruled out the jurisdiction of English courts. In 2020, the Liège Court of Appeal held that Belgian courts did not have jurisdiction to hear the dispute pursuant to the forum selection clause contained in Unilever's GTCs. Tilman challenged the Liège Court of Appeal's judgment before the Supreme Court.

Legal Issue

Article 23(1)(a) of the Lugano II Convention provides that if the parties, one or more of whom is domiciled in a State bound by this Convention, agreed in writing that a court of a State bound by this Convention is to have jurisdiction over any disputes that arose in connection with a particular relationship, that court will have jurisdiction. Article 23(2) of the Lugano II Convention specifies that "[a]*ny communication by electronic means which provides a durable record of the agreement shall be equivalent to 'writing'*". The Lugano II Convention extends the rules contained in Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (the ***Brussels I Regulation***) to Iceland, Norway and Switzerland. Article 23 of the Lugano II Convention and its counterpart of the Brussels I Regulation are substantially identical. Similar rules on the prorogation of jurisdiction are contained in Article 25 of Regulation (EU) No 1215/2012 of 12 December 2012 on jurisdiction and the enforcement of judgments in civil and commercial matters (the ***Brussels Ibis Regulation***) which succeeded the Brussels I Regulation to improve and facilitate the free circulation of judgments and to enhance access to justice.

In a judgment of 21 May 2015 (C-322/14, *Jaouad El Majdoub v CarsOnTheWeb.Deutschland GmbH*), the CJEU held that 'click-wrapping' satisfies the conditions of Article 23(2) of the Brussels I Regulation. Click-wrapping is a technique whereby a buyer ticks a box indicating that he/she accepts the seller's GTCs before finalising a purchase. A buyer will generally be able to consult and print the seller's GTCs by

clicking on a link which enables them to be displayed in a new window. In this respect, the CJEU considered that the condition that the method should provide a durable record of the agreement was met, because it allowed for the printing and saving of the GTCs before the conclusion of the agreement.

However, the service agreement between Tilman and Unilever did not make use of the click-wrapping technique. According to Tilman, the Liège Court of Appeal wrongly likened the service agreement to an online contract which can validly refer the buyer to GTCs accessible through a hyperlink. In this case, Tilman argued, it cannot be inferred from the execution of an agreement referring to Unilever's GTCs by way of a hyperlink that Tilman validly consented to the forum clause contained in the agreement.

Uncertain about how to apply the CJEU's past case law, the Supreme Court stayed the proceedings and submitted the following question to the CJEU for a preliminary ruling:

> *Does a jurisdiction clause contained in general terms and conditions to which a written agreement refers by way of a hyperlink to a website, which if accessed allows to read, download and print those general terms and conditions, but where the party against which this jurisdiction clause is enforced has not been invited to accept those general terms and conditions by ticking a box on the website, satisfy the conditions of Article 23(1)(a) and 23(2) of the Lugano II Convention?*

Conclusion

The impact of the CJEU's upcoming judgment will be more profound than the terms of the request for a preliminary ruling would seem to suggest. On the one hand, the judgment will affect the way businesses integrate their GTCs – an overwhelming majority of which contain forum selection clauses – in their B2B commercial contracts.

On the other hand, its impact will not only be felt for contracts falling within the scope of the Lugano II Convention, but also for contracts falling within the scope of the Brussels Ibis Regulation. In practice, the CJEU's ruling will affect all GTCs providing for the jurisdiction of (an) EU-based court(s), regardless of the domicile of the parties that concluded them, as well as all GTCs providing conferring jurisdiction on (a) court(s) based in the EU, Denmark, Iceland, Norway and/or Switzerland, if one or more of the parties that concluded them are domiciled in a State bound by the Lugano II Convention.

COMPETITION LAW

Belgian Competition Authority Clears Hospitals Merger

On 30 June 2021, the Belgian Competition Authority (*Belgische Mededingingsautoriteit / Autorité belge de la Concurrence* - ***BCA***) cleared a merger between three Brussels-based hospitals: (i) *Cliniques Universitaires de Bruxelles - Hôpital Erasme / Universitaire Klinieken Brussel - Erasmusziekenhuis*; (ii) *Institut Jules Bordet / Jules Bordet Instituut*; and (iii) *Hôpital Universitaire des Enfants Reine Fabiola / Universitair Kinderziekenhuis Koningin Fabiola*. These hospitals will form one group called *Grand hôpital universitaire de Bruxelles* (***GHUB***). GHUB will have legal personality and will be in charge of the strategy and operation of all three hospitals.

Although a law was recently adopted that exempts local hospitals networks, called "loco-regional clinical hospital networks", from the application of the Belgian merger control rules (*See*, this Newsletter, Volume 2021, No. 3, p. 4), this particular merger did not benefit from this exemption. For reasons that it did not explain in its decision, the BCA found that the transaction did not qualify as a "loco-regional clinical hospital network" under Article 14/1 of Coordinated Act of 10 July 2008 on hospitals and other health care institutions.

This transaction was cleared under the simplified procedure.

Draft Bill to Implement Directive 2019/633 on Unfair Trading Practices in the Agricultural and Food Supply Chain

On Friday 4 June 2021, the Federal Council of Ministers (*Ministerraad / Conseil des Ministres*) approved a draft bill that will implement Directive (EU) 2019/633 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain.

The bill is now being reviewed by the Council of State and will require a second approval by the Council of Ministers prior to its submission to Parliament.

Belgium missed the deadline of 1 May 2021 for the adoption and publication of implementing legislation of Directive 2019/633. It may still succeed in meeting the deadline for entry into force of the implementing legislation, which is 1 November 2021.

Belgian Competition Authority Clears Acquisition of Mobile Vikings by Proximus

On 31 May 2021, the Competition College (*Mededingingscollege / Collège de la concurrence*) of the Belgian Competition Authority (*Belgische Mededingingsautoriteit / Autorité belge de la Concurrence* - ***BCA***) unconditionally cleared the acquisition of mobile telecommunications operator Mobile Vikings NV (***Mobile Vikings***) by Belgium's incumbent telecommunications operator Proximus NV (***Proximus***).

Proximus offers a full range of electronic communications services at both wholesale and retail level, including fixed and mobile telecommunications, voice and data services, primarily in Belgium. Proximus is a mobile network operator (***MNO***), which offers mobile telecommunications services in reliance on its own mobile network. Proximus is also active in international wholesale electronic communications services ("international carrier's carrier services") and provides a range of IT services and other support services.

Mobile Vikings currently forms part of the DPG Group, which is a media group active in Belgium, Denmark and the Netherlands. Mobile Vikings offers mobile telecommunications services (voice, text messages and data) under the brands "Mobile Vikings" and "JIM Mobile". Mobile Vikings is a mobile virtual network operator (***MVNO***) and provides mobile telecommunications services on the Belgian market without owning a telecommunications network of its own. Its mobile services rely on an MVNO agreement which it concluded with MNO Orange Belgium.

The competition prosecutor (*auditeur / auditeur*) of the BCA in charge of the case found that the transaction was horizontal and affected (i) the Belgian retail market for the provision of mobile telephony services; (ii) the Belgian retail market for the provision of fixed telephony services; (iii) the Belgian wholesale market for fixed network call termination services; (iv) the Belgian wholesale market for call termination and call hosting to non-geographic numbers; (v) the Belgian wholesale market for call termination on fixed networks; and (vi) the Belgian wholesale market for call termination on mobile networks. However, the competition prosecutor reached the conclusion that the transaction would not lead to a significant impediment of effective competition in any of these markets. For its part, the Competition College of the BCA considered the analysis of the competition prosecutor to be "*thorough*", agreed with it, and cleared the transaction without conditions.

Interestingly, the Belgian Institute for Postal Services and Telecommunications (***BIPT***), Belgium's federal telecommunications regulator, had recommended to the BCA not to authorise the transaction. Among other objections, the BIPT considered Mobile Vikings to be a dynamic player (a "maverick") and a close competitor of Proximus on the "*highly concentrated retail market for mobile telephony services*". However, the Competition College disagreed and considered that both players were not close competitors, that Mobile Vikings was not a significant competitive force on the mobile retail market, and that its role would further decrease in the future. Likewise, the Competition College disagreed with the BIPT's assessment that the transaction would potentially increase prices that are "*already higher*" in Belgium. After stating that, "*given the high prices in Belgium*", its assessment must be guided primarily by the evolution of retail prices for mobile telephony services, the Competition College found that "[a]*fter an extensive economic analysis, the competition prosecutor has concluded that the incentive for parties to increase prices post-transaction is not substantially increased*".

The Competition College also rejected the BIPT's finding that the transaction will lead to a "*consolidation of Proximus' position as market leader in the mobile market*". According to the Competition College, the "*limited increments*" in terms of market shares and HHI values post-transaction "*already give a first indication of the absence of significant anticompetitive effects of the transaction*". The Competition College also considered Orange (for Belgium) and Telenet (for Flanders) to be the closest followers of the merged entity and the "*strongest growers in the mobile market*".

In its assessment, the Competition College relied on the statement made by DPG Group during the hearing that it no longer considers its business objectives for Mobile Vikings to be achievable despite the investments made. The Competition College also stressed DPG Group's statement that it was not prepared to make further investments or wait for better results, "*as the BIPT may deem necessary*". Finally, the Competition College underlined that, besides Proximus, Orange was the only candidate willing to acquire Mobile Vikings. According to the Competition College, this "*seems to imply that, at least for the time being, a takeover of Mobile Vikings does not fit into the strategy of other (potential) players with ambitions in the Belgian mobile market, in particular the recent newcomers Cegeka/Citymesh and Youfone, which are mentioned by the notifying party as a sign that the Belgian mobile market is competitive*".

DATA PROTECTION

In Belgian Case Involving Facebook Court of Justice of European Union Clarifies When Supervisory Authorities Can Derogate from One-Stop-Shop Principle

On 15 June 2021, the Court of Justice of the European Union (***CJEU***) handed down a judgment in which it detailed the circumstances in which a national Supervisory Authority (***SA***) can exercise its power to bring an alleged infringement of General Data Protection Regulation (EU) 2016/679 (the ***GDPR***) to court, even though that authority is not the Lead Supervisory Authority (***LSA***) with regard to the specific processing of personal data at issue. The judgment provides important clarifications on the functioning of the "one-stop shop" mechanism under the GDPR and the possibility for national SAs to bring an action in court outside the scope of this mechanism.

Background

The question arose in proceedings initiated in September 2015 by the President of the former Belgian Privacy Commission against Facebook before the Dutch-language Court of First Instance of Brussels (*Nederlandstalige Rechtbank van Eerste Aanleg te Brussel / Tribunal de première instance néerlandophone de Bruxelles* - the ***Court of First Instance***). Facebook Ireland, Facebook Inc. and Facebook Belgium (the ***Facebook Group***) had allegedly infringed Belgian data protection rules, principally by collecting and using information on the browsing behaviour of internet users, both Facebook account holders and others, by means of various technologies, including cookies, social plug-ins and pixels.

On 16 February 2018, the Court of First Instance ruled that Facebook's cookies (and similar technologies) infringed Belgian data protection laws. Moreover, it held that Facebook had failed to inform Belgian internet users adequately regarding the collection and use of the information concerned (*see*, VBB Client Alert here). The Court of First Instance accepted territorial jurisdiction over the Facebook Group (even though Facebook's main establishment is located in another Member State) and held that it was necessary for the Belgian Privacy Commission to be able to bring an action before the national court in order to have effective supervisory powers. The Facebook Group appealed the judgment to the Brussels Court of Appeal (*Hof van Beroep te Brussel / Cour d'Appel de Bruxelles* - the ***Court of Appeal***). The Belgian Data Protection Authority (***DPA***) acts as the legal successor to the President of the former Privacy Commission in the appeal procedure.

Request for Preliminary Ruling to CJEU

The Court of Appeal made a request for a preliminary ruling to the CJEU. It concerns the "one-stop shop" mechanism created by the GDPR. Under this mechanism, the SA of the location where a company has its EU headquarters (*i.e.*, the Lead Supervisory Authority or ***LSA***) is competent to decide on matters relating to cross-border processing of personal data (Article 56.1 GDPR). The Court of Appeal sought to know whether and to what extent the Belgian DPA could have competence in this cross-border case in which Facebook Ireland had been identified as the controller of the data concerned. In the case at hand, the Irish DPA is the LSA and the competent authority to bring injunction proceedings subject to review by the Irish courts.

CJEU Judgment: When Can SA Which Is Not LSA Start Legal Proceedings Against Controller of Personal Data For Alleged Infringements of GDPR?

In its judgment, the CJEU points out that the competence of SAs to adopt decisions on cross-border processing activities must be exercised with due regard to the cooperation and consistency procedures provided for by the GDPR. In general, the "one-stop shop" mechanism requires close, sincere and effective cooperation between SAs, in order to ensure a consistent and homogeneous protection of the data protection rules. The mechanism guarantees the competence of the LSA for the adoption of a decision finding that a cross-border processing activity infringes the GDPR. The competence of the other SAs concerned to adopt such a decision, even provisionally, is only allowed in exceptional cases. However, given the need for "*sincere*

and effective cooperation between supervisory authorities", the LSA cannot ignore the views of the other SAs. Any relevant and reasoned objection made by one of the other SAs has the effect of "blocking", at least temporarily, the adoption of the draft decision of the LSA.

Second, for an SA that is not the LSA to exercise its power to initiate or engage in legal proceedings with regard to cross-border processing, it is not a prerequisite that the controller in question has a main establishment or other establishment on the territory of that Member State.

Third, this SA can exercise its power both against the main establishment of the controller which is located in that authority's own Member State and against another establishment of that controller, provided that the object of the legal proceedings is a processing of data carried out in the context of the activities of that establishment and that that authority is competent to exercise that power. The CJEU adds that the exercise of this power implies the applicability of the GDPR. In the case at hand, since the activities of the establishment of the Facebook Group located in Belgium are inextricably linked with the processing of personal data at issue in the main proceedings, with respect to which Facebook Ireland is the controller within the EU, that processing is carried out "in the context of the activities of an establishment of the controller" and, therefore, falls within the scope of the GDPR.

Fourth, the CJEU considers that the proceedings were initiated before the entry into application of the GDPR and continued after the GDPR had come into force. In such a case, the CJEU holds that the action may be continued, under EU law, on the basis of the provisions of the former Data Protection Directive 95/46/EC. In addition, that action may be brought by that authority with respect to infringements committed *after* the entry into force of the GDPR, provided that: (i) the authority is permitted under the GDPR to adopt a decision notwithstanding the "one-stop-shop mechanism" (*e.g.*, in case of a purely local breach or in order to adopt an urgent, provisional measure); and (ii) the cooperation and consistency procedures provided for by the GDPR are respected.

Finally, the CJEU recognises the direct effect of the provision of the GDPR under which each Member State is to provide by law that its SA is to have the power to bring infringements of the GDPR to the attention of the judicial authorities and, when appropriate, to initiate or otherwise engage in legal proceedings. Consequently, such an authority may rely on that provision to bring or continue a legal action against private parties, even if that provision has not been specifically implemented in the legislation of the Member State concerned.

The full judgment of the CJEU is available here.

Employer's Communication on Circumstances of Dismissal Gives Rise to Reprimand by Belgian Data Protection Authority

On 1 June 2021, the Litigation Chamber (*Geschillenkamer/Chambre Contentieuse* – the ***Litigation Chamber***) of the Belgian Data Protection Authority (*Gegevensbeschermingsautoriteit/Autorité de protection des données* – the ***DPA***) issued a decision in which it held that the internal communications made by an employer concerning the reasons and circumstances of the dismissal of former employees infringed General Data Protection Regulation (EU) 2016/679 (the ***GDPR***) because the communications were not limited to what is necessary to inform the remaining staff of the employees' departure.

On 26 November 2019, two former employees (the ***complainants***) lodged a complaint with the DPA regarding the internal e-mail communications made by their former employer to the remaining staff about the complainants' dismissal and the circumstances that gave rise to the dismissal. The complainants alleged that the communications gave rise to a violation of the GDPR and one of them requested financial compensation for the breach.

In its decision, the Litigation Chamber examined whether the communications complied with the principle of data minimisation, enshrined in Article 5(1)(c) of the GDPR, which requires that personal data collected must be adequate, relevant and limited to what is necessary for the purposes for which they are processed. In particular, the DPA analysed whether the purpose of the processing of personal data could not reasonably be achieved by other means.

With regard to the first complaint, the DPA noted that the e-mail in question informed the remaining staff that the collaboration with the first complainant had been termi-

nated and that the first complainant would therefore no longer be present at the workplace. On that basis, the DPA concluded that the communication was limited to factual information which the DPA considered appropriate and proportionate to the aim pursued, notably informing the other employees that an employee's contract had been terminated. As a result, the DPA found that there was no violation of the GDPR.

The e-mail concerning the dismissal of the second complainant explained not only that the collaboration with the second complainant had been terminated but also that the decision to end the collaboration had been taken after three written warnings and performance reviews. While the employer argued that this information was provided to demonstrate compliance with internal dismissal procedures, the DPA considered that the reference to the number of warnings and performance reviews was not adequate, relevant and limited to what is necessary for the purpose of communicating the departure of an employee as part of the firm's human resources policy. Accordingly, the DPA decided to issue a reprimand to the employer for violating Article 5(1)(c) of the GDPR.

Finally, the Litigation Chamber decided to reject the second complainant's request to obtain financial compensation, indicating that the DPA does not have the power to grant financial compensation for a breach of the GDPR.

The DPA decision is available in Dutch (here) and in French (here).

European Commission Adopts Model Clauses for International Transfers and Processor Agreements

On 4 June 2021, the European Commission published two Implementing Decisions including model clauses that demonstrate compliance with General Data Protection Regulation (EU) 2016/679 (the GDPR). The first decision adopts new standard contractual clauses for the transfer of personal data to third countries (the Transfer SCCs) (Commission Implementing Decision (EU) 2021/914). The second decision contains a set of model clauses that can be used between controllers and processors (the Processor Clauses) (Commission Implementing Decision (EU) 2021/915).

Standard Contractual Clauses for International Transfers

More Situations Covered, More Flexibility and More Legal Certainty

The Transfer SCCs allow EU controllers and processors to transfer personal data to third countries outside the EEA which have not been recognised as providing an adequate level of protection for personal data (Article 46 GDPR). Compared to previous versions of the SCCs, the new Transfer SCCs provide for increased flexibility and additional legal certainty in accordance with the recent case law of the Court of Justice of the European Union (***CJEU***).

Through a modular approach, the Transfer SCCs cover additional situations that were not addressed by previous versions. For instance, the new Transfer SCCs can be used when the exporting party falls within the scope of the GDPR, even if the controller that is responsible for the data being exported is not established in the EU. In particular, the Transfer SCCs set out the following modules, which can be combined in a single agreement:

- From a controller (in the EU) to another controller (outside the EU);
- From a controller (in the EU) to a processor (outside the EU);
- From a processor (in the EU) to another processor (outside the EU); and
- From a processor (in the EU) to its appointing controller (outside the EU).

The parties to the transfer must select the applicable modules and identify the parties which are exporting or importing the personal data. The Transfer SCCs can be used by multiple parties and include arrangements for new parties acceding to the Transfer SCCs. This can be useful for intra-group transfers if a new subsidiary is established, and that subsidiary has to comply with intra-group data transfer arrangements with its overseas parent company.

In addition, the Commission emphasised that the SCCs reflect the requirements under the GDPR and take account of the CJEU's judgment in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (case

C-311/18) (***Schrems II***). While the CJEU stopped short of invalidating the current SCCs, individual contracts that include these clauses are liable to annulment if the parties fail to use the SCCs in compliance with the CJEU case law. Because the new Transfer SCCs explicitly take account of the CJEU case law, they increase legal certainty for international transfers of personal data.

More Work to Implement and Monitor

The modular approach provides more options for parties to cover complex international transfers with SCCs. However, in order for organisations to pick the correct modules and complete the information required to adapt the SCCs to the situation at hand, they must have a good view of their international transfers, be able to determine the parties involved, identify their role as either controller or processor in the transfer, outline the categories of data concerned and the reasons for the transfer, and identify the sub-processors and the applicable security measures.

Additionally, the parties to the Transfer SCCs should use "reasonable efforts" to ensure that each data importer is able to satisfy the obligations under the Transfer SCCs. It means that parties must be able to assess whether the contractual obligations under the Transfer SCCs are compatible with the local law in the importing countries. If necessary, the parties to the Transfer SCCs must adopt supplementary safeguards.

Lastly, the data importer may be required to challenge a request by a public authority if it considers that such a request is unlawful pursuant to the law of the importing country or under international law obligations and the principles of international comity.

What to Do With Existing SCCs?

The new Transfer SCCs will be effective on 27 June 2021 and will apply to data processors and controllers subject to the GDPR. After 27 September 2021, no new contracts can be concluded on the basis of the previous versions of the SCCs. Previous versions of the SCCs in contracts signed before that date will have to be replaced by the new Transfer SCCs (or another transfer mechanism authorised under the GDPR) by 27 December 2022.

The Transfer SCCs are available here.

Standard Contractual Clauses between Controllers and Data Processors

The Commission also published Processor Clauses, *i.e.*, SCCs between controllers and data processors under Article 28 of the GDPR. Their use is not mandatory. Parties can still rely on their own clauses in processor agreements provided these meet the mandatory requirements of Article 28 of the GDPR.

The Processor Clauses are available here.

European Commission Initiates Infringement Proceedings against Belgium

On 9 June 2021, the European Commission (the ***Commission***) started infringement proceedings against Belgium concerning the independence of the Belgian Data Protection Authority (*Gegevensbeschermingsautoriteit/Autorité de protection des données* – the ***DPA***).

Pursuant to Article 52 of General Data Protection Regulation (EU) 2016/679 (the ***GDPR***), Supervisory Authorities (***SAs***) should act with complete independence in performing their tasks and exercising their powers under the GDPR. They should remain free from any external direct or indirect influence which is liable to affect their decisions.

The Commissioner for Justice, Didier Reynders, expressed his concerns on the independence of the Belgian DPA in a letter of March 2021, since some of the DPA's members either report to a management committee depending on the Belgian government, take part in governmental projects on Covid-19 contact tracing, or are members of the Information Security Committee. The information provided by the Belgian competent authorities in response to that letter did not alleviate the Commission's concerns.

Consequently, the Commission sent a letter of formal notice on 9 June 2021 initiating infringement proceedings. Belgium has two months to reply and clarify the measures which it has taken to ensure full independence of the Belgian DPA. If these measures are deemed insufficient, the Commission may take the next step in the infringement procedure and send Belgium a reasoned opinion.

The Commission's press release on the subject can be found here.

EU Adequacy Decisions for EU-UK Personal Data Flows

On 28 June 2021, the European Commission adopted two adequacy decisions for the transfer of personal data from the EU and EEA to the United Kingdom following the agreed post-Brexit transition period. The two adequacy decisions allow personal data transfers under: (i) General Data Protection Regulation (EU) 2016/679 (the ***GDPR***) (this adequacy decision is available here); and (ii) Directive 2016/680 (the ***Law Enforcement Directive***) (this adequacy decision is available here). The decisions came days before the transitional agreement under the EU-UK Cooperation Agreement was set to expire on 30 June 2021 and ensure that personal data can be transferred freely from the EU/EEA to the UK for the next four years.

Following its thorough assessment of the UK's practice on the protection of personal data including rules on the access to data by public authorities, the Commission reached the conclusion that the UK's data protection system continues to be based on the same rules that were applicable while the UK was still a Member State of the EU. The Commission's decision means that the UK's data protection standards are considered "adequate", pursuant to Article 45 of the GDPR. However, the Commission warns that it will monitor the UK's data protection standards and it may reconsider the adequacy finding if the UK were to deviate from the current data protection standards in place for EU citizens.

The UK incorporated the principles, rights and obligations of the GDPR and the Law Enforcement Directive into the UK Data Protection Act 2018 (the ***DPA 2018***) which governs the protection of personal data in the UK post-Brexit. As a result, the UK's data protection regime largely resembles that of the EU. Nevertheless, there were some hurdles for the Commission in arriving at an adequacy finding.

One of these hurdles consists of a recent UK Court of Appeal judgment in *R (Open Rights Group and The3million) v Secretary of State for the Home Department and Others [2021] EWCA Civ 800* which held that the immigration exemption in the DPA 2018 is unlawful. The Commission pragmatically excluded the UK Immigration Control from the scope of its adequacy finding and stated that it would reassess the need for this exclusion once the underlying position has been remedied under UK law.

Another hurdle relates to potential developments in UK law. For this reason, both adequacy decisions contain a "sunset-clause" limiting the validity of the EU adequacy decision until 27 June 2025. After this date, the Commission can extend the adequacy finding if it is able to ascertain that UK rules continue to ensure an adequate level of data protection.

European Data Protection Board Adopts Final Recommendations on Supplementary Measures for International Transfers

On 21 June 2021, the European Data Protection Board (the ***EDPB***) published the final version of its Recommendations 01/2020 on measures to supplement transfer tools. A draft of the Recommendations was adopted on 10 November 2020, following the *Schrems II* judgment of the Court of Justice of the European Union (the ***CJEU***) (*See*, this Newsletter, Volume 2020, No. 11, p. 14). In this judgment, the CJEU held that organisations relying on Standard Contractual Clauses (***SCC***) must assess, as a safeguard and on a case-by-case basis, whether the SCC should be supplemented by additional measures. The EDPB's Recommendations aim to assist data exporters in their duty to implement the supplementary measures in cases where the destination country's level of protection is not equivalent to that applying to the European Economic Area (the ***EEA***).

The final version of the Recommendations addresses feedback received during the public consultation but still retains the six-step process outlined in the first draft of the Recommendations, which can be summarised as follows:

- Organisations should record and map all transfers of personal data outside of the EU, taking into account onward transfers and remote access from third countries (*e.g.*, storage in a cloud outside the EEA). They should also verify that the data transferred is adequate, relevant, and limited to what is necessary.

- Organisations should verify the transfer tools relied on for each transfer. The final draft of the Recommendations provides a broader scope for derogations under General Data Protection Regulation 2016/679 (the ***GDPR***) by stating that the derogations must be used "*in a way which does not contradict the very nature of the derogations as being exceptions from the rule… Derogations cannot become "the rule" in practice but need to be restricted to specific situations.*"

- The Recommendations emphasise the importance of assessing the law and practice of the third country to determine whether they impinge upon the effectiveness of the appropriate safeguards. An organisation's assessment must include whether authorities in the third country may seek access to the specific data transferred.

- Organisations should also assess whether the laws of the third country diminish in practice the ability of data subjects to exercise their rights under the transfer tool. The EU Charter of Fundamental Rights should be used as a reference when assessing whether authorities' powers to access data exceed what is necessary and proportionate, and whether there is effective redress for data subjects. When accessing the risk related to relevant transfers, organisations should use relevant, objective, reliable, verifiable, and publicly available information, but may consider the practical experience of the importer.

- If the legal assessment concludes that the destination country's laws and/or practices impinge on transfer safeguards, organisations should implement supplementary measures to ensure adequate protection. Possible measures may be of a technical, contractual and organisational nature.

- The Recommendations require that organisations should take any formal procedural step necessary to implement the supplementary measures.

- Finally, the Recommendations emphasise the importance of re-evaluating data transfer arrangements and monitoring any developments. Supervisory authorities will continue to monitor the application of the GDPR and enforce it. Following an investigation or complaint, the supervisory authorities may suspend or prohibit data transfers that they find cannot ensure an equivalent level of protection. Supervisory authorities will continue developing guidance for exporters and ensuring that EU data protection law is applied consistently.

The final version of Recommendations 1/2020 is available here.

European Data Protection Board Publishes Annual Report 2020

On 2 June 2021, the European Data Protection Board (***EDPB***) published its Annual Report for 2020 (the ***Annual Report***) which contains four highlights.

First, the EDPB contributed to the European Commission's evaluation of General Data Protection Regulation (EU) 2016/679 (the ***GDPR***). The EDPB found that the GDPR's application has been successful since it has strengthened data protection as a fundamental right and increased the global visibility of the EU legal framework. On the other hand, the EDPB identified certain challenges, such as insufficient resources for the Supervisory Authorities (***SAs***), as well as inconsistencies in national procedures that impact the cooperation mechanism between different SAs.

Second, the EDPB issued guidance on the numerous measures taken by Member States to monitor, contain and mitigate the spread of the Covid-19 virus with regard to the contact-tracing apps, the use of location data, the processing of personal data in the context of the reopening of borders, and the processing of health data for research purposes (*See*, this Newsletter, Volume 2020, No. 4, at p. 12).

Third, the EDPB issued multiple guidance documents relating to international personal data flows following the Schrems II judgment of the Court of Justice of the European Union (***CJEU***) (*See*, our note on the *Schrems II* judgment here). More concretely, the EDPB issued answers to frequently asked questions (*See*, this Newsletter, Volume 2020, No. 8, at p. 7); Recommendations 01/2020 on measures that supplement transfer tools, which should ensure compliance with the level of protection required under EU law; and Recommendations 02/2020 on European Essential Guarantees for surveillance measures allowing access to personal data by public authorities in third countries (*See*, our client alert on draft Recommendations 01/2020 and 02/2020 here; the EDPB adopted a final version of Recommendations 01/2020 on 18 June 2020, *see*, above).

Fourth, the EDPB adopted its first dispute resolution decision on the basis of Article 65 of the GDPR. The binding decision concerned a dispute that arose following a draft decision by the Irish Data Protection Commission acting as a lead SA regarding Twitter International Company and the

subsequent relevant and reasoned objections expressed by a number of concerned SAs (*See*, this Newsletter, Volume 2020, No. 12, at p. 10).

Other activities undertaken by the EDPB in 2020 include the adoption of ten guidelines on topics such as consent (*See*, this Newsletter, Volume 2020, No. 5, at p. 12), the concepts of controller and processor in the GDPR (*See*, this Newsletter, Volume 2020, No. 9, at p. 8) and the targeting of social media users (*See*, this Newsletter, Volume 2021, No. 4, at p. 7). Furthermore, the EDPB adopted opinions to ensure the consistent application of the GDPR across the EEA. These are issued upon request of a national SA before it can adopt a decision that has cross-border implications.

Last, in early 2021, the EDPB adopted its two-year work programme for 2021-2022 (*See*, this Newsletter, Volume 2021, No. 3, at p. 12), which follows the priorities set out in the EDPB Strategy for 2021-2023 (*See*, this Newsletter, Volume 2020, No. 12, at p. 9). The EDPB's strategic objectives are: (i) enhancing harmonisation and facilitating compliance; (ii) supporting effective enforcement and efficient cooperation between national SAs; (iii) preserving fundamental rights in the face of new technologies; and (iv) considering the global dimension of data protection.

The EDPB's Annual Report can be consulted here.

Belgian Data Protection Authority Publishes Annual Report 2020

On 11 June 2021, the Belgian Data Protection Authority (*Gegevensbeschermingsautoriteit/Autorité de protection des données* – the ***DPA***) published its annual report 2020 (the ***Annual Report***).

The DPA created a dedicated Covid-19 page on its website (available in Dutch and in French) which it regularly updates with new guidelines and answers to frequently asked questions from both citizens and data controllers. The DPA also issued numerous opinions on normative texts setting up data processing operations by the Belgian State to combat the current health crisis (a list of opinions related to Covid-19 is available in Dutch and in French).

Importantly, at the beginning of 2020, the DPA adopted its strategic plan for 2020-2025 (*See*, this Newsletter, Volume 2019, No. 12, at p. 7; the final version of the strategic plan can be found here). In line with its priorities for the period 2020-2025, the DPA published a comprehensive recommendation on data processed for direct marketing purposes, a recurring topic in information and mediation requests, but also in complaints and inspections (*See*, this Newsletter, Volume 2020, No. 3, at p. 8). The DPA also focused on data protection online and fined Google Belgium for misinterpreting the right to be forgotten (*See*, this Newsletter, Volume 2020, No. 7, at p. 10).

The number of complaints doubled in the course of the year. In addition to general questions on the GDPR, data subject rights and privacy principles, complaints, mediation requests and information requests were mainly related to direct marketing, consumer data and surveillance cameras.

The DPA's Annual Report can be consulted in Dutch (here) and in French (here).

INSOLVENCY

Term of Pre-packaged Insolvency Procedure and Enhanced Accessibility to Judicial Reorganisation Procedure Extended

On 29 June 2021, the term of the pre-packaged insolvency procedure that was temporarily introduced in Belgium by the Law modifying Book XX of the Code of Economic Law was extended until 16 July 2022 (*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***).

The Law, which initially entered into force on 26 March 2021, introduced (i) a pre-packaged insolvency procedure; and (ii) certain measures to make the judicial reorganisation procedure more accessible (*See*, this Newsletter, Volume 2021, No. 3, p. 14). The Law aimed to provide economically viable companies with a temporary legal framework to help them in their economic recovery from the Covid-19 crisis.

Pre-Packaged Insolvency Procedure

The procedure allows for a fast-track negotiation process with a debtor's most important creditors without the negative consequences associated with the publicity and burdensome procedure of a conventional judicial reorganisation procedure.

A court-appointed judicial officer must assist the company in the negotiations with its creditors. The negotiations are designed to work out the terms of (i) an amicable agreement with at least two of the debtor's creditors (which will only bind the creditors who are a party to the agreement); or (ii) a collective restructuring plan (binding all creditors if approved by the majority of the creditors who represent the majority of the total debt of the debtor).

If the negotiations are successful, the "pre-packaged" agreement or 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

In addition, the Law also temporarily abolished 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.

INTELLECTUAL PROPERTY

At Request of Antwerp Enterprise Court, Court of Justice of European Union Analyses Communications to Public for Copyright Purposes and Recognises Right To Sue of Non-Practising Entities

On 17 June 2021, the Court of Justice of the European Union (***CJEU***) largely followed Advocate General (***AG***) Szpunar's opinion in case C-597/19 *Mircom International Content Management & Consulting (MICM) Limited v Tel¬enet BVBA*. The CJEU held that making protected works available on a peer-to-peer network amounts to making the work "available to the public" within the meaning of Article 3(1) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (***InfoSoc Directive***). The CJEU added that right holders do not have actually to exercise their rights to benefit from the remedies provided for by EU Law. Finally, the CJEU held that the Infosoc Directive does not preclude the systematic registration and the communication of the users' IP addresses if these engaged in infringing activities on peer-to-peer networks.

Factual Background and Procedure

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

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

CJEU's Reasoning

On the first question, the CJEU confirmed that pursuant to Article 3 of the Infosoc Directive, uploading pieces of a digital file containing protected work to a peer-to-peer network amounts to making that work available to the public. There is no minimum threshold of pieces to download to determine whether the resulting upload and transmission cause the work to be made available as long as the user gives public access to a protected work.

Second, the CJEU held, contrary to AG Szpunar's opinion, that Article 4(b) of the Enforcement Directive must be interpreted as meaning that a right holder bringing an action as the assignee of the rights can benefit from the remedies under Chapter 2 of that Directive.

Third, the CJEU clarified that it is for the referring court to ensure that requests made under the Enforcement Directive are justified, proportionate and not abusive. The CJEU added that a high level of protection of intellectual property in the internal market has to be guaranteed.

Fourth, the CJEU also held that Article 6(1)(f) of the GDPR read together with Article 15(1) of Directive 2002/58 con-

cerning the processing of personal data and the protection of privacy in the electronic communication sector (***Directive 2002/58***) do not preclude the rightsholder's systematic registration of IP addresses of the users engaging in infringing activities in peer-to-peer networks, or the communication of the names and postal addresses of the users to the right holder in the context of an action for damages. However, any such requests for the data must be justified, proportionate and not abusive.

The CJEU's judgment can be found here.

Court of Justice of European Union Explains Limitations Placed by Database Rights on Search Engines

On 3 June 2021, the Court of Justice of the European Union (***CJEU***) delivered a judgment on the *sui generis* database right in case C-762/19 SIA '*CV-Online Latvia' v SIA Melons*. The CJEU followed AG Szpunar's opinion in holding that displaying a third party's database through a specialised search engine and redirecting users to the original website amounts to measures of reutilisation and extraction prohibited by Article 7(1) of Directive 96/9 of 11 March 1996 on the legal protec¬tion of databases (the ***Database Directive***).

Factual Background and Procedure

SIA CV Online Latvia (***CV Online***), a Latvian Company, oper¬ates a website containing a regularly updated database of job notices published by employers. The database uses meta tags, making it easier for search engines to identify and index the contents of each page. SIA Melons (***Melons***), another Latvian company, operates a search engine spe¬cialising in notices of employment. In its search results, this search engine refers to the websites on which the informa¬tion sought was initially published by way of hyperlinks. For its searches, Melons also showed results contained in CV Online's website. CV Online sued Melon for extracting and re-using a substantial part of the contents of its database and thus infringing its sui generis database right.

The Riga Regional Court referred two questions to the CJEU for a preliminary ruling. First, whether the use of a hyperlink to redirect end users to a website where they can consult a database of job advertisements, can be interpreted as a reutilisation of the database by another form of transmission within the definition of Article 7(2)(b) of the Database Directive. Second, whether the information containing the meta tags shown in the search engine can be defined as "extraction" within the meaning of Article 7(2)(a) of the Database Directive, more specifically, as the permanent or temporary transfer of all or a substantial part of the database's content to another medium by any means or form.

CJEU's Reasoning

First, the CJEU rephrased the questions referred and interpreted broadly the notions of reutilisation and extraction. The CJEU held that the transfer of substantial contents of the databases that makes these available to the public without the database owner's consent amounts to measures of extraction and re-utilisation of databases prohibited by Article 7(1) of the Database Directive. This is only the case if such a transfer has the effect of depriving the owner of the expected income to recover its investments costs.

Second, the CJEU reconciled the interests of the database owner with the advantages brought by the content aggregators such as that of contributing to the development of the EU information market. According to the CJEU, a fair balance must be struck between the protection afforded by the Database Directive and unfair competition. The national court should consider whether the extraction and reutilisation will prevent the database owner from recovering their investment by jeopardising the revenues resulting from the database exploitation.

The CJEU's Judgment can be found here.

Court of Justice of European Union Details Conditions for Liability of Platform Operators for Illegal User Content

On 22 June 2021, the Court of Justice of the European Union (***CJEU***) ruled on the liability of platform operators for copyright infringing user content pursuant to Article 3 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***) in joined cases C-682/18 *YouTube* and C-683/19 *Cyando*.

Factual Background and Procedure

In the first case, Frank Peterson, a music producer, brought legal proceedings before the Hamburg Higher Regional Court against YouTube and its parent company Google, for making available to the public without his authorisation musical works in which he claimed to have the rights. The second case involved Elsevier Inc. (***Elsevier***), a publishing group, which had brought proceedings before the Munich Regional Court to obtain an injunction against Cyando AG (***Cyando***) for uploading without authorisation works in which it claimed to have exclusive rights. Both cases were appealed to Germany's Federal Court of Justice which in turn referred several questions to the CJEU for a preliminary ruling.

The first question was whether platform operators make work available to the public within the meaning of Article 3 of the Infosoc Directive by having users upload copyright-protected materials without the holder's authorisation. The second question was whether the platform operators can rely on the exemptions for hosting providers of Article 14(1) of Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (***E-Commerce Directive***). The third question referred was whether right holders can obtain an injunction against the platform operators under Article 8(3) of the Infosoc Directive.

CJEU's Reasoning

On the first question, the CJEU held that operators do not generally make a communication to the public, unless they contribute to making the illegal content accessible. There must therefore be an element of knowledge on the part of the operators to consider that they make a communication to the public within the meaning of Article 3 of the Infosoc Directive. The CJEU went on to provide a non-exhaustive and non-cumulative list of criteria to determine whether platform operators contribute to the illegal communication. For instance, the CJEU considered whether they take technological measures to counter copyright infringements, if they intervene in the creation of content or monitor it before uploading it, if the operators warn the users that their account will be blocked in case of repeated infringements, or if they base their financial model on the illegal sharing of protected content.

Second, the CJEU analysed the role played by platform operators. It held that to benefit from the exemption, platform operators cannot play an active role of the kind that gives them control or actual knowledge over the users' content. The CJEU cited two conditions that cause the requirements of Article 14 of the E-Commerce Directive to apply: (i) the operators should not have actual knowledge of the illegal activity; and (ii) when the operators become aware of such illegal activity, they must act expeditiously to remove or disable access to that information.

Third, the CJEU held that Article 8(3) of the Infosoc Directive must be interpreted as not precluding a national law under which a right holder cannot obtain an injunction against a platform operator whose services were used by a third party to infringe their rights if that platform intermediary had no knowledge or awareness of the infringement within the meaning of Article 14 of the E-Commerce Directive.

The CJEU's judgment can be found here.

LITIGATION

Brussels Court of First Instance Finds Against Belgian Federal and Regional Governments in Climate Litigation

On 17 June 2021, the French-language Brussels Court of First Instance (*Franstalige Rechtbank van Eerste Aanleg te Brussel / Tribunal de première instance francophone de Bruxelles* - the ***Court***) handed down its judgment in climate litigation finding that the federal government and the governments of the three regions (*i.e.*, Brussels, Flanders and Wallonia) breached Article 1382, Civil Code governing tort liability and Articles 2 and 8, European Convention on Human Rights (***ECHR***) by failing to take the necessary measures to limit the adverse effects of climate change on the country's population.

On 27 April 2015, the environmental non-profit association "Klimaatzaak" representing 58,000 Belgian citizens (the ***claimants***) brought an action against the Belgian federal government and the governments of the three regions, alleging that these authorities breached their general duty of care and the citizens' human rights by failing to implement commitments to fight climate change.

In its judgment, the Court first addressed the admissibility of the action and held that the 58,000 citizens showed a personal and direct interest in the action in view of the genuine threat of climate change for the daily lives of citizens in Belgium and elsewhere. In addition, the Court considered that the non-profit association "Klimaatzaak" had an independent personal and direct interest in the action in accordance with its statutory object which aims to combat climate change.

On the merits, the Court considered that both the federal government and each of the governments of the three regions were individually liable for failing to meet their climate obligations. The Court based its reasoning on three findings.

First, Belgium showed mixed results in terms of reducing greenhouse gas emissions (the ***GHG emissions***) and therefore failed to meet international, European and national GHG emissions reduction targets. More specifically, Belgium failed to comply with:

- international targets laid down in the 2012 Doha Amendment to the Kyoto Protocol to the United National Framework Convention on Climate Change of 1997;
- European targets set out in Decision No 406/2009 of the European Parliament and of the Council of 23 April 2009 on the effort of Member States to reduce their greenhouse gas emissions;
- internal targets which Belgian authorities set for themselves.

In addition, experts projected that Belgium will also not meet the targets for 2030 set by EU Regulation 2018/842 of 30 May 2018 on binding annual greenhouse gas emission reductions by Member States from 2021 to 2030, even if additional internal policies were implemented.

Second, the authorities failed to implement a strong climate governance. In particular, the Court considered that since climate policy is a competence shared between the federal government and the governments of each of the three regions, these entities should have taken appropriate coordinated actions to meet their climate obligations.

Third, the Court noted that Belgium received repeated warnings from the European Union concerning its failure to satisfy its climate commitments.

These findings, together with the fact that the Belgian authorities had full knowledge of the risks of climate change on the country's population, led the Court to conclude that neither the federal government, nor the governments of the three regions had acted with the degree of care and diligence required by Article 1382, Civil Code. In addition, the Court held that the same authorities breached the claimants' rights to life and right to privacy enshrined in Articles 2 and 8 of the ECHR. In that respect the Court stressed that the authorities did not take appropriate measures to prevent the risks and adverse consequences of climate change on the claimants' life and privacy.

The Court nonetheless rejected the claimants' request for an injunction to reduce the GHG emissions further by 48% (or at least by 42%) in 2025, by 65% (or at least by 55%) in 2030, and by 100% in 2050. It held that whilst it could be determined that the federal government and the government of the three regions were liable for a breach of their obligations, the principle of separation of powers did not allow the Court to intervene in political decisions and set specific GHG emission reduction targets.

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