October 2024

VBB on Belgian Business Law

Issue Highlights

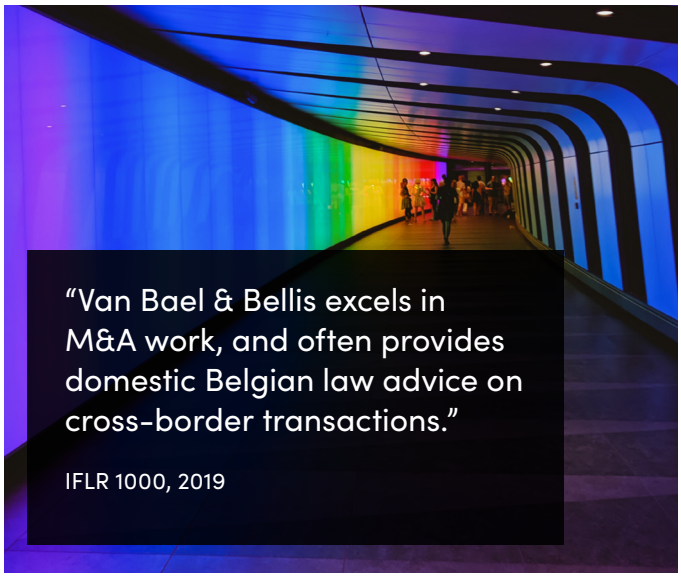
"Van Bael & Bellis' Belgian competition law practice [...] is a well-established force in high-stakes, reputationally-sensitive antitrust investigations."

Legal 500, 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
Fax: +32 (0)2 640 64 99

vbb@vbb.com
www.vbb.com

COMMERCIAL LAW

Bill Governing Personal Security Interests (Book 9 of New Civil Code) Is Submitted to Federal Chamber of Representatives for Second Time

On 24 September 2024, Private Members' Bill 56K0261 was submitted to the federal Chamber of Representatives to modify and update the statutory provisions governing personal security interests (*Wetsvoorstel houdende titel 1 "Persoonlijke zekerheden" van boek 9 "Zekerheden" van het Burgerlijk Wetboek / Proposition de loi portant le titre 1er "Les sûretés personnelles" du livre 9 "Les sûretés" du Code civil* - the ***Bill***). The Bill forms part of the broader reform of the Civil Code and constitutes the first part of Book 9 regarding "Securities".

The Bill reproduces Private Members' Bill 55K3825 which had been submitted to the federal Chamber of Representatives on 7 February 2024 (*See*, this Newsletter, Volume 2024, No. 3). The Council of State issued its opinion on that bill (available here) on 23 May 2024, *i.e.*, the day on which the Parliament was dissolved in view of the federal elections of 9 June 2024. Bill 55K3825 lapsed but was resuscitated by the Bill which took on board some of the Council of State's recommendations as follows:

- The Bill clarifies that the existence of a personal security cannot be presumed. A clear expression of intent is required for a personal security to exist. The party asserting the existence of personal security bears the burden of proof.

- Contrary to bill 55K3825, the Bill provides that suretyship for all debts (*borgtocht voor alle schuldvorderingen / cautionnement pour toutes créances*) does not extend to debts transferred to a principal debtor as a result of a contribution or transfer of a branch of activities (*bedrijfstak / branche d'activités*).

- The Bill extends the surety's right of recourse against the principal debtor to situations in which the principal debtor is not liable to the creditor due to the inexistence or breach of its corporate object but limits the recourse to the amount of the principal debtor's enrichment.

The Bill is available here.

Council of European Union Adopts New Product Liability Directive

On 10 October 2024, the Council of the European Union (***Council***) adopted the Directive on liability for defective products and repealing Council Directive 85/374/EEC (***New Product Liability Directive***). The New Product Liability Directive revises the existing rules on product liability to enhance the protection of consumers and other natural persons and to adapt the regime to the digital age.

Background

The existing EU product liability framework dates back to 1985 and provides consumers and other natural persons with a means to seek compensation for damage caused by defective products that are commercialised in the European Economic Area, regardless of negligence or fault on the part of their producer. However, these rules have failed to address the challenges posed by technological developments, including artificial intelligence (***AI***), circular economy models, and increasingly complex global supply chains.

What is new?

The New Product Liability Directive introduces the following changes to EU product liability rules:

- **Extended scope of products**: The New Product Liability Directive covers a wider range of "products" than the current product liability directive (Directive 85/374/EEC), including software (such as operating systems, firmware, and AI systems) and digital services integrated into or inter-connected with the product.

- **Broader range of damage covered**: Compensation claims now extend to additional types of damage, such as medically recognised psychological injury, and destruction or corruption of data that are not used for professional purposes.

- **Presumption of defect or causal link**: To ease the claimant's burden of proof, the New Product Liability Directive contains specific presumptions that allow for the assumption of defectiveness or

COMMERCIAL LAW

the existence of a causal link between a defect and damage. For instance, in cases in which technical or scientific complexity makes proving a defect excessively difficult, these presumptions can support the claimant's case. However, these presumptions remain subject to rebuttal.

- **Assessment of defect**: Under the New Product Liability Directive, a product is considered defective when it "*does not provide the safety that a person is entitled to expect or that is required under* [EU] *or national law*". When assessing the existence of a defect, courts must consider the following criteria: (i) the product's presentation and inherent characteristics; (ii) its reasonably foreseeable use; (iii) the product's ability to learn or acquire new features after it is placed on the market or put into service; (iv) the reasonably foreseeable effect of other products on the product in question (*e.g.*, within a smart home system); (v) the moment in time when the product was placed on the market or put into service or when the product leaves the manufacturer's control; (vi) compliance with relevant product safety requirements (including safety-relevant cybersecurity requirements); (vii) any recall or other relevant interventions related to product safety by the competent authority or an economic operator; (viii) the specific needs of the product's intended users; and (ix) the nature of products whose very purpose is to prevent damage (*e.g.*, warning mechanisms like smoke alarms).

- **Extended group of potentially liable persons**: Liability now extends to more entities within the supply chain, including those that provide components and associated services.

Next steps

The New Product Liability Directive is expected to be published in the Official Journal of the European Union, after which EU Member States will have two years to transpose it into national law.

The New Product Liability Directive as adopted by the Council is available here.

COMPETITION LAW

New President Belgian Competition Authority Speaks Out on Priorities and Areas of Concern

Axel Desmedt became the new President of the Belgian Competition Authority (***BCA***) on 1 March 2024 (*See*, this Newsletter, Volume 2024, No. 2). Following a period of deliberate silence in order to allow himself time to settle in and attend to urgent matters, Mr. Desmedt recently gave public indications regarding the direction of travel of the BCA under his stewardship at the Belgian University Foundation (*Universitaire Stichting / Fondation universitaire*) on 11 October 2024 and at Informa's Digital Challenges in Competition Law on 17 October 2024. While not all the points which Mr. Desmedt mentioned are new, some reflect fresh ideas or imply an intensified focus on specific matters by the BCA.

- *Call-in Merger Control Powers* – Emulating the example of his counterparts in other national competition authorities, including the Dutch Autoriteit Consument & Markt, Mr. Desmedt advocates for a change in the law that would confer on the BCA the power to "call in" and review mergers that would not normally qualify for competition scrutiny because they do not satisfy the financial thresholds for doing so. His position was prompted by the judgment delivered by the Court of Justice of the European Union (***CJEU***) on 3 September 2024, in *Illumina Grail*. The CJEU held in that case that Article 22 of the EU Merger Control Regulation does not provide the statutory basis for mergers over which Member States have no jurisdiction under their national merger control regime to be referred for review to the European Commission (the ***Commission***). The call-in powers, which already exist in several EU Member States, would remedy what Mr. Desmedt and others consider an "enforcement gap" and enable the BCA to examine such mergers itself or request that the Commission carry out such a review.

- *New Competition Tool* – Mr. Desmedt is also a proponent of a New Competition Tool (***NCT***) that would enable the BCA to tackle market distortions even if no infringement of the competition rules by specific parties was established. Such an instrument is already on the statute books in Germany and has been called for by, once more, the President of the "*Autoriteit Consument & Markt*" in The Netherlands. Mr. Desmedt pointed out that Articles V.3 and V.4, Code of Economic Law, created a precursor to the NCT on a smaller scale in that these provisions only apply to pricing issues and solely allow for the adoption of temporary measures.

- *Coordination with European Commission and Member State Competition Authorities* – For Mr. Desmedt, coordinating enforcement activities with other relevant competition authorities will often be key to reaching a successful outcome in a given case.

- *Support for European Commission Policies* – An important part of the BCA's new tasks is to assist the Commission in applying the Digital Markets Act (*See*, this Newsletter, Volume 2024, No. 3; and Belgian Antitrust Watch of 25 June 2024) and the Foreign Subsidies Regulation. The BCA's brochure explaining the DMA will be published shortly.

- *Telecommunications* – Mr. Desmedt, a former member of the executive board of the Belgian Institute for Post and Telecommunications, will continue to keep a watchful eye on the telecommunications sector, which is not only an important industry in its own right but also creates the foundations for economic activity overall. Important matters include new market entry and the proposed network infrastructure cooperation for the roll-out of new fibre networks (*See*, this Newsletter, Volume 2024, No. 6-7).

- *Cooperation with Other Regulators* – Smooth cooperation with other regulators responsible for postal services and telecommunications, energy,

COMPETITION LAW

financial services, and data protection is crucial and will require cooperation agreements and the adaptation of the regulatory framework.

- *Sector Inquiries* – Mr. Desmedt confirms that the BCA is gearing up for its first sector inquiry but refuses to identify its target.

- *Internal Organisation* – The BCA has undergone a transformation, both in terms of numbers and in organisational outlook, (which includes an expanded team of economists; the creation of specialist teams dealing with pharmaceuticals, food, and digital markets; and digitalised case management, archiving, and knowledge management). Further work is needed on the legal service; the human resources function; communications; and information technology.

- *Evergreens* – The BCA will continue to spend time and efforts on the enforcement of competition policy in traditional areas such as resale price maintenance.

CONSUMER LAW

Council of European Union Adopts Position on New Measures to Facilitate Alternative Dispute Resolution for Consumers

See Litigation section.

DATA PROTECTION

Court of Justice of European Union Holds that Legitimate Interests Can Encompass Purely Commercial Interests

On 4 October 2024, the Court of Justice of the European Union (the ***CJEU***) handed down its judgment in case C-621/22, *Koninklijke Nederlandse Lawn Tennisbond*, in response to a reference for a preliminary ruling by the District Court of Amsterdam (the ***Referring Court***). The CJEU held that a wide range of interests may qualify as '*legitimate interests*' under the General Data Protection Regulation (***GDPR***) and that purely commercial interests should not be excluded from that category.

Background of Case

In 2019, the Dutch Data Protection Authority (***Dutch DPA***) fined the Royal Dutch Lawn Tennis Association (***KNLTB***) EUR 525,000 for unlawfully disclosing personal data of its members to two sponsors for marketing activities in exchange for payment. The Dutch DPA found that KNLTB had infringed the GDPR by disclosing members' personal data without their consent and without any legal basis.

Before the Referring Court, KNLTB contended that the disclosure of the members' personal data was based on their legitimate interest, as established by Article 6(1)(f) GDPR, aimed at strengthening the relationship between the association and its members by offering them value-added benefits, like discounts and promotional offers from partners, which made tennis more affordable and accessible. By contrast, the Dutch DPA maintained that for an interest to be legitimate, it should be enshrined in and determined by law. According to KNLTB, commercial interests did not meet this test.

The Referring Court stayed the procedure and sought guidance from the CJEU on three issues: (i) the definition of '*legitimate interests*'; (ii) the question as to whether such interests must exclusively pertain to the law; and (iii) whether any interest can be legitimate as long as it does not breach the law.

CJEU's Judgment – Three-step Test

The Court reiterated the three cumulative conditions contained in Article 6(1)(f) GDPR to assess whether the reliance on legitimate interests is lawful.

First, *there must be a pursuit of a legitimate interest*. The CJEU previously held that, in the absence of a definition of this concept in the GDPR, a wide range of interests can be regarded as "legitimate". These interests need not necessarily be established and determined by law, but they should be lawful. The CJEU confirmed that the commercial interests of a controller consisting in the promotion and sale of advertising space for marketing purposes may be regarded as a set of legitimate interests (*see* para. 73; by analogy, C-131/12, *Google Spain and Google*).

Second, the processing of personal data must be *necessary*. This means that the claimed legitimate data processing interests could not have been achieved just as effectively by other means that are less restrictive of the fundamental rights and freedoms of data subjects. The CJEU suggested that KNLTB could have informed its members about the data disclosure and sought their prior consent. This approach would have minimised the intrusion into their right to protection of the confidentiality of their personal data, while still allowing KNLTB to pursue its legitimate interests in an equally efficient manner.

Third, the *balancing of interests must point to the protection of the claimed legitimate interests*. This condition entails a balancing the opposing rights and interests at issue which depends on the specific circumstances of the case and should be assessed by the Referring Court. While leaving this concrete assessment to the Referring Court, the CJEU nonetheless mentioned the importance of considering whether aspiring members could have reasonably expected that their data would be shared with third

DATA PROTECTION

parties for marketing purposes. The CJEU also raised concerns about the nature of the third parties involved – specifically providers of games of chance and casino games – whose marketing and promotional activities do not fit in a relevant and appropriate relationship between the data subjects and the controllers.

Takeaways

This decision offers considerable relief for organisations relying on legitimate interests as a legal basis for data processing. At the same time, the CJEU's clarifications leave little room for doubt regarding the likely unfavourable outcome of this case for KNLTB.

National data protection authorities are now expected to follow unreservedly the CJEU's position that legitimate interests can encompass purely commercial interests, a position that was already held by most DPAs. Still, stakeholders must remember that to rely on Article 6(1)(f) GDPR, their data processing must not only be lawful but must also be strictly necessary and carefully balanced against the fundamental rights and interests of data subjects. Conveniently, the European Data Protection Board recently offered guidelines on processing personal data based on legitimate interests under Article 6(1)(f) GDPR (*see* below).

European Data Protection Board Publishes Draft Guidelines on Legitimate Interests

On 8 October 2024, the European Data Protection Board (***EDPB***) published draft guidelines 1/2024 on the processing of personal data based on legitimate interests (the ***Guidelines***) under Article 6(1)(f) GDPR.

Legitimate Interests Cannot Be Default Option

'Legitimate interests' are likely the preferred choice of many controllers among the six lawful bases for data processing contained in Article 6(1) General Data Protection Regulation (***GDPR***). They provide the GDPR with a degree of flexibility and, contrary to the notion of 'consent' (Article 6(1)(a) GDPR), do not require an opt-in and easy withdrawal options for data subjects.

However, the EDPB points out that legitimate interests should not be considered a default option or an option of last resort. Identifying a legitimate interest alone does not satisfy the requirements of Article 6(1)(f) GDPR. As is illustrated by the judgment of the Court of Justice of the European Union in *Koninklijke Nederlandse Lawn Tennisbond* (discussed above), controllers must still assess whether the three cumulative conditions for lawful processing are satisfied.

- The interests pursued by the controller, or third party, must be *legitimate*;
- The processing must be *necessary* to achieve these legitimate interests; and
- The interests or fundamental freedoms and rights of the data subjects *should not outweigh these interests*.

Controllers must document this assessment from the outset, in line with the accountability principle set out in Article 5(2) GDPR.

Detailed Guidance on Three-step Test

The Guidelines offer further clarifications regarding each of the components of the test.

First, the interest must be legitimate. While this concept is not defined in the GDPR, the CJEU has recognised various interests as 'legitimate', including the access to online information, operating public websites, bringing damage claims, and improving products. The Guidelines clarify that, to be legitimate, an interest must be: (i) lawful; (ii) clearly and precisely articulated; and (iii) real and present, rather than speculative.

Second, the processing must be strictly necessary—not merely useful—for pursuing the identified legitimate interest. This requirement means that if the controller has reasonable, less intrusive alternatives available, that would be just as effective, the processing is unlikely to be considered 'necessary'.

DATA PROTECTION

Finally, the interests of the controller must not be overridden by the interests or fundamental rights and freedoms of the data subjects. This step requires balancing between the legitimate interests pursued against the impact on the fundamental rights and freedoms of the data subjects. The Guidelines explain that these include the right to liberty and security, freedom of expression and information, freedom of thought, conscience and religion, and freedom of assembly and association (para.37 of the Guidelines). In many cases, this balancing exercise will constitute the central element of the three-step test. The purpose of this exercise is not to avoid any impact on the interests and rights of the data subjects, but to avoid a *disproportionate* impact. According to the Guidelines, the impact of the processing on the data subject may be influenced by (i) the nature of the data to be processed (for example, whether special categories of data are involved); (ii) the context of the processing (its scale, the controller's status, and the degree of accessibility of the data); and (iii) the further consequences which the processing may have (such as the possible production of legal effects for the data subject and potential financial loss).

Additionally, the "reasonable expectation" of the data subjects must play a significant role in the controller's assessment. The Guidelines provide a non-exhaustive list of contextual factors for assessing such expectations: (i) characteristics of the relationship or the service provided (*e.g.*, the proximity of the relationship, and the nature of the service); and (ii) the characteristics of the "average" data subject whose personal data is to be processed (*e.g.*, age, status as a public figure, and other attributes).

If the assessment finds that the legitimate interests pursued outweigh the data subject's interests, rights, and freedoms, the processing is allowed to proceed. If that is not the case, then the controller must implement mitigating measures to balance the impact on data subjects. These measures should go beyond the steps resulting from the application of the standard GDPR requirements.

Practical Applications

The Guidelines also address specific situations for the processing of legitimate interests, including:

- Processing of children's personal data: Children's interests will often take precedence over those of the controller. The EDPB considers that extensive profiling and targeted advertising typically do not align with the obligation to protect children.

- Processing for direct marketing purposes: Direct marketing can qualify as a legitimate interest, but its lawfulness depends on the reasonable expectations of data subjects and the compliance with relevant laws, such as the e-Privacy Directive, which takes precedence over the GDPR in this area. It follows that if consent is required pursuant to the e-Privacy Directive, legitimate interests cannot be relied on as a legal basis.

Helpful Clarification, but Notable Omission

The guidelines lack specific guidance on the use of artificial intelligence (***AI***). As businesses increasingly rely on customer data for model training, guidance on whether legitimate interests can serve as a basis for such processing is necessary. The Belgian Data Protection Authority's decision of 15 March 2024 (*See*, this Newsletter, Volume 2024, No. 6-7) touched on this possibility, but the EDPB has yet to address the use of AI directly. The upcoming EDPB Guidelines on Generative AI, scheduled in the EDPB Work Programme 2024-2025, will hopefully bring clarity. In the meantime, businesses seeking to leverage customer data for AI must determine for themselves whether their processing meets the requirements of the three-step test.

The Guidelines 01/2024 will be subject to public consultation until 20 November 2024.

DATA PROTECTION

Court of Justice of European Union Limits Processing of Sensitive Personal Data for Targeted Advertising

On 4 October 2024, the Court of Justice of the European Union (***CJEU***) handed down its judgment in case C-446/21, *Maximilian Schrems v Meta Platforms Ireland Ltd*, clarifying the limitations on processing personal and sensitive data for advertising purposes. This judgment follows a reference for a preliminary ruling by the Austrian Supreme Court seeking guidance on data processing practices for personalised advertising.

Background of Case

After the General Data Protection Regulation (***GDPR***) took effect in 2018, Meta Platforms Ireland (***Meta***) updated Facebook's terms of use, requiring user consent for continued platform access. Facebook's primary revenue model depends on personalised advertising tailored to users' preferences and online behaviour, tracked both on Facebook and across third-party sites.

In this case, Maximilian Schrems, who had intentionally restricted the amount of information on his Facebook account, initially accepted Facebook's terms. However, he later observed advertisements targeting LGBTQ+ individuals, even though he had not explicitly shared information about his sexual orientation on his profile. Meta explained that its algorithms inferred interests from his activity and associations, not from overt data regarding his sexual orientation. However, Schrems argued that this processing violated the GDPR as it involved sensitive data for which use no explicit consent had been given. His claim was dismissed by lower courts, prompting him to appeal to the Austrian Supreme Court, which sought the CJEU's interpretation on the following issues:

- Whether GDPR's data minimisation principle allows the unrestricted processing of personal data for advertising purposes, without limitation on data type or retention period; and

- Whether a user's partial disclosure of sensitive information (*e.g.*, sexual orientation) permits further processing of similar data by the platform.

CJEU's Judgment

Data Minimisation

In its judgment, the CJEU stressed that the data minimisation principle prohibits data controllers from processing the personal data of users without clear restrictions on the duration and type of data used. The CJEU specified that data processing should be limited to data that is adequate, relevant, and strictly necessary for the intended purpose. Any retention of data must also be limited to what is essential for the specific processing activity. Accordingly, the indiscriminate data collection for targeted advertising, whether gathered on or off the platform, violates the GDPR if the data type or retention period is unrestricted.

Disclosure

In response to the second question, the CJEU held that Article 9(2)(e) GDPR, which allows processing of sensitive data "manifestly" disclosed by the data subject, should be narrowly interpreted. This provision requires a clear intention by the data subject to make his or her sensitive data publicly accessible. The CJEU noted that, based on the context of the panel in which Mr. Schrems had referred to his homosexuality, it could indeed be inferred that Mr. Schrems had openly disclosed his sexual orientation. However, this disclosure alone did not constitute permission to process other, related data. Therefore, the CJEU held that an online platform cannot use information regarding an individual's sexual orientation gathered outside the platform, including from third-party sources, to aggregate and analyse the data and on that basis deliver personalised advertising.

The case will return to Austria's Supreme Court, which will apply the principles of the CJEU's judgment to the facts of the case.

DATA PROTECTION

European Data Protection Board Offers Updated Guidance on Scope of Tracking Requirements of ePrivacy Directive

On 7 October 2024, the European Data Protection Board (***EDPB***) adopted Guidelines 2/2023 (***Guidelines***) establishing a three-criterion test to determine when the use of tracking technologies requires consent pursuant to Article 5(3) of Directive 2002/58/EC concerning privacy in electronic communications (***ePrivacy Directive***).

The first criterion probes whether operations involve "information". The EDPB deliberately uses a broader scope than personal data, reflecting the ePrivacy Directive's goal of protecting users' private sphere. According to the EDPB, the protection extends to any information stored in terminal equipment, regardless of its connection to an identified or identifiable person. The Court of Justice of the European Union (Case C-673/17, *Planet 49*, at para. 70) confirmed this interpretation, ruling that protection is afforded to all information stored in terminal equipment, including hidden identifiers and similar devices entering users' equipment without their knowledge. The criterion encompasses information regardless of its origin - whether entered by users, pre-installed by manufacturers, or placed by third parties. Even scenarios involving non-personal data that intrude into users' private sphere, such as malware storage, fall within the scope of protection.

The second criterion contains two components: "terminal equipment" and connection to a "public communications network". Terminal equipment must be used with publicly available electronic communications services and must be connected or connectable to a public network interface. The EDPB confirms that this covers both traditional devices like smartphones and computers, and emerging technologies such as connected cars or smart glasses. The public communications network requirement encompasses any transmission system allowing signal conveyance, including satellite, mobile, and cable networks. Importantly, the EDPB clarifies that networks available to a limited public subset, such as paying subscribers, still qualify as public networks.

The third criterion addresses "storage" and "gaining access" as separate triggering events. Storage occurs when information lands on any physical electronic storage medium within the user's terminal equipment, regardless of duration. This encompasses temporary caching in RAM, permanent storage on hard drives, or any intermediate solution. "Gaining access" covers scenarios in which entities take steps to retrieve information from terminal equipment. The EDPB specifically explains that tracking pixels exemplify indirect access: when a pixel is embedded in a website or e-mail, it instructs the user's device to establish communication with the pixel's host automatically. This communication transmits information stored on the user's terminal equipment back to the host. The fact that the entity instructing the sending of information (the website owner) might differ from the entity receiving it (the advertising service) does not prevent Article 5(3) from applying.

Applying these criteria, tracking pixels embedded in websites or e-mails are in scope both when stored on users' devices and when transmitting data to their host. IP-based tracking requires consent when companies cannot ensure that the IP address originates from sources other than users' terminal equipment, though addresses processed through carrier-grade network address translation may be out of scope.

While providing technical clarity, the Guidelines deliberately avoid addressing exceptions to consent requirements, leaving this type of analysis to a case-by-case assessment under national implementing laws. The Guidelines supplement the Article 29 Working Party's 2014 opinion on device fingerprinting, ensuring privacy rules remain effective as tracking technologies evolve.

The Guidelines can be consulted here.

FOREIGN DIRECT INVESTMENT

European Commission Publishes Fourth Annual Report on Foreign Direct Investment Screening

On 17 October 2024, the European Commission (the ***Commission***) published its fourth Annual Report (the ***Report***) on the screening of foreign direct investments (***FDI***) in the European Union (the ***EU***). The Report addresses FDI trends in the EU, as well as legislative developments and FDI screening activities in the Member States. In addition, the Report offers data on the functioning of the EU cooperation mechanism on FDI screening which was created by the FDI Screening Regulation (the ***Regulation***). The Report also discusses the proposed revision of the Regulation (*See*, this Newsletter, Volume 2024, No. 1).

Nearly All Member States Now Screen FDI

The Report indicates that, as of 31 March 2024, 24 Member States had an FDI screening mechanism. Eight of those Member States only adopted their mechanism in 2023 or later. This group of Member States includes Belgium, where the FDI screening mechanism entered into force on 1 July 2023 (*See*, this Newsletter, Volume 2023, No. 5). The Interfederal Screening Committee (*Interfederale Screeningscommissie / Comité de Filtrage Interfédéral* – the ***ISC***) recently published its first annual report on FDI screening in Belgium (the ***Belgian Report***; *See*, this Newsletter, Volume 2024, No. 9). The Report adds that the remaining three Member States initiated a consultative or legislative process expected to result in the adoption of a new mechanism.

Smooth Process for Most, but More Notifications and Mandatory Measures

The Report indicates that Member States handled 1,808 FDI notifications and *ex officio* investigations in 2023, as opposed to 1,444 in 2022. Of these, 56% were subject to formal screening. This is a slight increase compared to 2022, when 55% of the cases were formally screened. These figures contrast with those of the Belgian Report, which does not mention any cases falling outside of the scope of the Belgian FDI screening mechanism.

In addition, the Report indicates that the vast majority of notified FDI cases were cleared without measures. However, the Report reflects a slight decrease in FDI cases cleared without measures in 2023 (85%) compared to 2022 (86%). In addition, the Report notes a slight increase in approved FDI subject to measures in 2023 (10%) compared to 2022 (9%). As was the case in previous years, only approximately 1% of transactions were blocked, and 4% of notifications were withdrawn. These figures again contrast with those of the Belgian Report, which mentions that the ISC did not block or subject any transactions to measures in its first year of operations.

Furthermore, the Report indicates that the Commission's close scrutiny of potentially harmful FDI remains limited to exceptional cases. Specifically, of the 488 cases shared within the EU cooperation mechanism in 2023, 92% were closed within 15 days, while just 8% prompted additional information requests and only 2% resulted in an opinion being issued by the Commission. This represents a slight decrease in FDI being looked at in more detail compared to 2022, when 87% out of 421 notifications shared within the EU cooperation mechanism were closed by the Commission within 15 days. Notwithstanding the increased scrutiny of FDI over the past years, the Report signals that the EU continues to be an open global investment environment.

Screened Investments

From the 488 cases shared within the EU cooperation mechanism in 2023, most FDI cases were in manufacturing (23%), ICT (21%), wholesale and retail (14%), financial activities (11%), professional services (*e.g.,* law, accounting, consultancy, and engineering) (11%), and energy (6%). This is very similar to the figures of 2022, when most FDI cases were also in manufacturing, ICT and wholesale and retail. Conversely, the sectors targeted by notifications under the Belgian FDI screening mechanism during the ISC's first year of operations were data (15.1%), healthcare (15.1%), digital infrastructure (11.6%), transport (10.5%) and electronic communications (8.1%).

FOREIGN DIRECT INVESTMENT

FDI in manufacturing (including aerospace, defence and semiconductors) and ICT accounted for most in-depth assessments by the Commission (39% and 24% respectively, which is similar to last year's figures of 59% and 23% respectively). Notably, FDI in wholesale and retail, professional services and financial activities was looked at in more detail, accounting for 10%, 10%, and 8% of the Commission's in-depth assessments.

The Report further mentions that of the 488 cases shared within the EU cooperation mechanism in 2023, FDI mostly originated in the United States (33%), the UK (12%), the United Arab Emirates (7%, as opposed to 3% in 2022), China (including Hong Kong, at 6%), Canada (5%) and Japan (4%). The remaining 33% of FDI originated in other countries, while this was 44% in 2022, pointing to a higher concentration of FDI originating in the top six countries of origin. These figures are broadly in line with those of the Belgian Report, which indicates that the majority of notified FDI in Belgium originated in the United States (43.4%) and the UK (29%).

Outlook

The EU FDI screening rules may soon be amended. In January 2024, the Commission tabled a proposal to modify the Regulation (*See*, this Newsletter, Volume 2024, No. 1). The proposed changes reflect new geopolitical and security challenges and address gaps and shortcomings identified during the application of the Regulation. The proposal, which is currently under review by the European Parliament and the Council of the EU, will make it compulsory for all Member States to have a national FDI screening mechanism. Additionally, it seeks to introduce a minimum level of harmonisation of national screening laws across the EU by (i) identifying a minimum sectoral scope for screening purposes; and (ii) harmonising FDI notifications through procedural improvements and increased accountability between the Member States and the Commission. The Commission expects the proposal to be approved in 2025 with the new rules to enter into force in 2026 or 2027.

The full Report can be consulted here.

INTELLECTUAL PROPERTY

Court of Justice of the European Union Delivers Landmark Judgment Rejecting the Application of the Reciprocity Clause of the Berne Convention

On 24 October 2024, the Court of Justice of the European Union (the ***CJEU***) delivered a judgment in the *Kwantum Nederland BV, Kwantum België BV v. Vitra Collections AG* case (C-227/23), rejecting the application of Article 2(7) of the Berne Convention for the Protection of Literary and Artistic Works (the ***Berne Convention***) to works of applied art originating from non-EU countries and authored by non-EU nationals. It follows that works of applied art of non-EU origin will qualify for copyright protection under the EU copyright system, provided the conditions for such protection are satisfied.

Background

This preliminary reference originates from a dispute between Vitra Collections AG (***Vitra***), a Swiss designer furniture manufacturer, and Kwantum Nederland BV and Kwantum België BV (together, ***Kwantum***), a retail chain selling interior design products. Vitra is a copyright holder of the Dining Sidechair Wood (the ***DSW chair***), originally created by the American spouses Charles and Ray Eames. It initiated an action against Kwantum alleging that a chair commercialised by the chain breached the intellectual property rights of Vitra. Kwantum argued that the material reciprocity clause of the Berne Convention should apply and that works of applied art of non-EU origin should only receive copyright protection if afforded equivalent protection in the third country concerned.

The matter reached the Dutch Supreme Court (the ***Referring Court***) which stayed the proceedings and referred preliminary questions to the CJEU regarding the interpretation of Article 2(7) of the Berne Convention and EU law, in particular the Charter of Fundamental Rights (the ***CFR***), Directive 2001/29 on the harmonisation of certain aspects of copyright and related rights in the information society (the ***Infosoc Directive***) and Article 351 of the Treaty on the Functioning of the European Union (the ***TFEU***).

CJEU Judgment

First, the CJEU clarified that any work commercialised in the internal market that meets the Infosoc Directive's definition of 'work' falls under the material scope of EU law, irrespective of the country of origin of the work and the nationality of its author. The CJEU's assessment of the applicability of the EU copyright protection to works of non-EU origin considered the scope and objectives of the Infosoc Directive.

As regards the application of the material reciprocity clause, the CJEU pointed out that the EU legislature necessarily took into account all the works for which protection was sought in the territory of the European Union. It did not lay down any criterion as to the country of origin of these works or the nationality of their author. The application of the material reciprocity clause by the Member States would go against the objective of the Directive to harmonise copyright protection in the internal market. The CJEU observed that any limitation of the right to protection of intellectual property under Article 17(2) CFR must be provided for by law and must be initiated at EU level.

The assessment of the CJEU is fully in line with the Opinion of Advocate General Szpunar delivered on 5 September 2024 (*See*, this Newsletter, Volume 2024, No. 9) and marks a significant development of EU copyright law. The implication of this judgment is particularly significant for non-EU authors, as it affords equal copyright protection at EU level, irrespective of whether the non-EU author is able to enforce the copyright in the country of origin concerned. This judgment may provide an attractive route of enforcement for non-EU authors subject to stricter copyright regimes.

The judgment can be found here (in English).

INTELLECTUAL PROPERTY

Court of Justice of the European Union Clarifies Cheating Software Does Not Constitute Copyright Infringement

On 17 October 2024, the Court of Justice of the European Union (the ***CJEU***) delivered a judgment in *Sony Computer Entertainment Europe Ltd v Datel Design and Development Ltd e.a,* (C-159/23) in which it clarified the scope of Directive 2009/24 of 23 April 2009 on the legal protection of computer programmes (***Computer Programmes Directive***).

Background

The dispute arose between Sony Computer Entertainment Europe Ltd (***Sony***), which commercialises PlayStation games consoles as well as games for those consoles, including the game "*MotorStorm:Arctic Edge*", and Datel Design and Development Ltd and Datel Direct Ltd (***Datel***). Datel develops, produces and distributes software and devices that are compatible with Sony's game consoles, including devices and software which present users with game options not provided at that stage of the game by Sony.

Before the German courts, Sony claimed that by means of Datel's devices and software users are able to alter the software which underpins the "*MotorStorm:Arctic Edge*" game, resulting in the infringement of Sony's copyright. Sony therefore sought the cessation of the marketing of those devices and software as well as compensation for the damage which it allegedly suffered. The dispute ended up before the German Federal Court of Justice (the ***Referring Court***) which referred a request for a preliminary ruling to the CJEU.

CJEU Judgment

The Referring Court asked if the Computer Programmes Directive covers the variable data transferred to a computer's RAM by a protected programme, used during the programme's operation. The CJEU concluded that this type of transfer is not protected under the Computer Programmes Directive, as it does not enable the reproduction or creation of the programme itself. Copyright protection for computer programmes is limited to the original intellectual creation found in the source and object codes, not in variable data or functionality.

The CJEU based this interpretation on Article 1 of the Computer Programmes Directive, which protects only the "expression in any form" of a programme, excluding ideas or principles, as long as the programme is original and reflects the author's intellectual creation. Thus, while the source and object codes are protected, elements like functionality and user interfaces that do not enable the reproduction or creation are not. Protecting functionality alone, the CJEU reasoned, would create monopolies over ideas and hinder technological progress.

This interpretation is in line with recital 15 of the Computer Programmes Directive, which specifies that infringement involves the unauthorised reproduction or transformation of the programme's code. The Computer Programmes Directive aims to protect programme authors from unauthorised reproductions, not from modifications that do not alter the core code.

In this case, Datel's software modified only variable data in the PSP console's RAM, affecting gameplay but not Sony's game code. The CJEU concluded that such temporary modifications, which do not reproduce or alter the original code, do not infringe copyright, allowing developers of "cheat" or modification software the legal freedom when their changes are temporary and do not impact the core source code.

The judgment can be found here in English.

LITIGATION

Council of European Union Adopts Position on New Measures to Facilitate Alternative Dispute Resolution for Consumers

On 20 September 2024, the Council of the European Union (the ***Council***) approved two legislative proposals presented by the European Commission (the ***Commission***) on 17 October 2023. They aim to adapt the alternative dispute resolution (***ADR***) framework to the challenges of a digital world. The European Parliament (the ***Parliament***) had adopted its first-reading position on 13 March 2024.

Background

As an alternative to court litigation, ADR mechanisms allow consumers to attempt to resolve their disputes with companies through ADR bodies (such as mediators or the ombudsman) or via the European online dispute resolution (***ODR***) platform (***ODR Platform***). In Belgium, ADR bodies include the Consumer Mediation Service, the Telecommunications Mediation Service, the Ombudsman Service for Energy and the Ombudsman for Trade.

ADR Directive

The Commission's first legislative proposal aims to revise Directive 2013/11/EU on alternative dispute resolution for consumer disputes (***ADR Directive***) to cover new kinds of unfair practices that can be resolved out of court (*e.g.*, misleading advertising and interfaces or unjustified geo-blocking mechanisms). It also proposes to include all dimensions of EU consumer protection laws and all types of companies, including non-EU traders.

The Council's position is to limit the scope of the ADR Directive to contractual disputes (which also include the stages leading up to the conclusion of a contract and following the termination of a contract) and to the European territory, leaving for each Member State to decide on the application of ADR procedures to disputes with third-country traders.

ODR Platform

The Commission's second legislative proposal is to adopt a Regulation on the discontinuation of the ODR Platform and replace it with a digital interactive tool that would ensure continuity and make ADR mechanisms easier to use, faster and more attractive for both consumers and business. In addition, the Commission's proposal contains several measures to protect the most vulnerable consumers that offer assistance with launching a case, translation aids and guidance throughout the procedure.

The Council's position clarifies that ADR should be accessible in both digital and non-digital formats to ensure a high level of consumer protection. The Council also provides that firms should inform consumers in advance when non-high-risk automated systems (*i.e.*, bots or artificial intelligence) are used in ADR decision-making processes, as is the case for high-risk systems covered by the Artificial Intelligence Act.

The Council further confirms the need to reduce the burden on all stakeholders and empowers the Commission to replace the existing ODR Platform with a new digital tool, within three months after the entry into force of the revised ADR Directive.

Next steps

ADR entities had until 1 November 2024 to submit their reports on the development and functioning of ADR mechanisms to the competent authorities.

The Council will now negotiate the final text of the proposals with the Parliament.

The Commission proposal on ADR is available here. The Commission proposal on the ODR Platform is available here.

Brussels
Glaverbel Building
Chaussée de La Hulpe 166
Terhulpsesteenweg
B-1170 Brussels
Belgium

Phone:+32 (0)2 647 73 50
Fax:+32 (0)2 640 64 99

Geneva
26, Bd des Philosophes
CH-1205 Geneva
Switzerland

Phone:+41 (0)22 320 90 20
Fax:+41 (0)22 320 94 20

London
Holborn Gate
330 High Holborn
London
WC1V 7QH
United Kingdom

Phone: +44 (0)20 7406 1471

VAN BAEL & BELLIS

www.vbb.com