Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

Data Protection & Cybersecurity

Second Edition

Belgium
Sidley Austin LLP

chambers.com

2019

Law and Practice

Contributed by Sidley Austin LLP

Contents

Sidley Austin LLP is a premier law firm with more than 2000 lawyers worldwide representing clients on complex transactional, regulatory and litigation matters spanning more than 40 legal disciplines. From our offices in the commercial, financial and regulatory centres of the world, we harness our knowledge to provide thoughtful and practical advice for the myriad legal and business challenges that our clients face. With a practice attuned to the ever-changing international landscape, Sidley's Data Privacy and Cyber Security practice represents and assists companies across a range of industries to comply with and address some of the most challenging matters concerning data protection, privacy, information security and incident response, data commercialisation, internet and computer law, IP, information management and records retention, e-commerce, consumer protection and cyber-crimes. Our team provides extensive cross-border support in developing and implementing global data protection programmes for clients with operations in Europe, Asia, the US and beyond.

Authors

Wim Nauwelaerts is well-versed on all aspects of EU and international data protection and privacy law. He has nearly 20 years' experience of assisting multinational organisations with various aspects of privacy, data protection and cybersecurity, including preparation for the EU General Data Protection Regulation (GDPR), data transfer strategies, data security and breach requirements, and compliance training. Wim also assists clients with contract negotiations and represents them before supervisory authorities. While Wim counsels clients in a variety of sectors, he has particular experience with life sciences, technology and new media clients, and frequently co-ordinates global privacy projects. He regularly assists clients in crafting and implementing comprehensive programmes as a critical step in helping to ensure that personal data is used appropriately and safeguarded against loss and unauthorised use or disclosure. Wimm is a member of the International Association of Privacy Professionals (IAPP) and is fluent in Dutch, English and French.

Lauren Cuyvers advises clients on a wide range of data protection, IT and cybersecurity matters including GDPR compliance, data-breach counselling and related pan-European litigation. Prior to joining Sidley in 2018, Lauren was an associate in the IP and data protection practices of other international law firms based in Brussels, where she advised and litigated for clients in the life sciences and media sectors in relation to IP and data protection matters. In 2014, Lauren interned at the Belgian Permanent Mission to the UN in New York and completed an LLM cum laude in IP and EU competition law. She is an IAPP member, a Certified Information Privacy Professional Europe and is fluent in Dutch, English and French.

1. Basic National Legal Regime

1.1 Laws

The Belgian Constitution sets out the rights to respect for private and family life and correspondence as fundamental human rights. In addition, a number of international instruments on privacy and data protection have direct effect and therefore individuals can rely on them before the Belgian courts, including:

- the Council of Europe Convention 108 on the Protection of Privacy and Trans-border Flows of Personal Data;
- the European Convention on Human Rights and Fundamental Freedoms (Article 8 on the right to respect for private and family life); and
- the Charter for Fundamental Rights of the European Union (Article 7 on the right to respect for private and family life and Article 8 on the right to the protection of personal data).

At national level, data protection law currently consists of three main sources of legislation, namely the Act on the Establishment of the Supervisory Authority of 3 December 2017 (the 'SA Act'), the Data Protection Act of 30 July 2018 (the 'DP Act') and the EU General Data Protection Regulation 2016/679 (the 'GDPR'), which is directly applicable in the Belgian legal system. The DP Act and SA Act were passed to supplement the GDPR further and replace the previous data protection law (which included the Data Protection Act of 8 December 1992). It is worth noting that, in addition to supplementing the GDPR, the DP Act also transposes the EU Law Enforcement Directive 2016/680 and covers data processing that falls outside of the GDPR's scope of application (such as data processing by intelligence agencies and the military).

These data protection laws are supplemented by specific legislation and collective labour agreements (CLAs), such as the new Act on the use of surveillance cameras (the 'Camera Act') and CLA No 68, which governs the use of CCTV systems in an employment context. E-privacy provisions found in Directive 2002/58/EC, such as cookie requirements, were implemented in the Belgian Act on Electronic Communications of 13 June 2005 (the 'Electronic Communications Act'). Belgium is divided into regions ('régions' in French, or 'gewesten' in Dutch) and communities ('communautés' or 'gemeenschappen'), which are competent to issue region- or community-specific supplementary legislation in the form of decrees or ordonnances.

There is no standalone or overarching law with regard to information security or cybersecurity, but the DP Act and SA Act contain general requirements, including notification requirements, which mirror the GDPR and in essence reflect the 72-hour notification period and related requirements. These requirements in the DP Act are also upheld for processing activities that do not reside within the scope of the GDPR, such as processing in the context of law enforcement. Furthermore, the Electronic Communications Act imposes specific reporting obligations on electronic communications service-providers in the case of a security breach.

1.2 Regulators

The main data protection regulator in Belgium is the Belgian Data Protection Authority. With the entry into force of the SA Act, the Data Protection Authority took over the role of the Belgian Privacy Commission as an independent institution overseeing compliance with the GDPR, the DP Act, the SA Act and other more specific legislation such as the Camera Act. The Data Protection Authority has residual competence over data protection matters, meaning that it has the authority to regulate such matters unless more specific legislation appoints a different regulatory authority. It has the authority to issue advice and guidance, to handle complaints and requests, to take enforcement action and to initiate investigations.

The Data Protection Authority consists of different actors, each of which play a specific role in the investigation of a data protection matter, such as the Frontline Service (performing a triage function to determine which complaints merit further investigation), the Inspection Body (mainly carrying out investigations) and the Dispute Resolution Chamber (where administrative proceedings are conducted). An investigation is usually triggered by a complaint or request submitted by an individual or other stakeholder, but could also be initiated by the Data Protection Authority on its own initiative. The Data Protection Authority was granted a diverse and more far-reaching set of powers after the SA Act entered into force, such as the power to conduct on-site investigations and audits, to interview and interrogate relevant individuals, to seize goods and IT systems, to request identification of relevant individuals, and "any other investigation, verification and interrogation that is deemed necessary to ascertain that applicable data protection principles are complied with."

The Belgian Institute for Postal Services and Telecommunications (the 'Institute') has the authority to oversee compliance with the Electronic Communications Act, including relevant e-privacy provisions, which do not involve processing of personal data. To assess compliance, the Institute may perform audits and initiate investigations (which can also be triggered by a complaint).

The Flemish Region has established a specific regulator to oversee data processing activities by Flemish public authorities by Decree of 18 July 2008, named the Flemish Supervisory Commission ('Vlaamse Toezichtscommissie'). Pursuant to this Decree, the Flemish Supervisory Commission has the same investigative powers granted to Supervisory Authorities by the GDPR, including the right to audit and access buildings, information and IT systems. Investigations are initiated in the same way as investigations before the Data Protection Authority, ie, following a complaint or upon the Flemish Supervisory Commission's own initiative. A Brussels and Walloon counterpart was established to oversee data processing within the Brussels Capital, Walloon Region and French-speaking Community (by these regions' public authorities). At this point in time, no law has been passed at regional level to grant similar investigative powers as was done for the Flemish Supervisory Commission.

1.3 Administration and Enforcement Process

The Data Protection Authority's investigative and/or corrective powers are usually triggered by a complaint or request filed with the Authority's Frontline Service ('Service de Première Ligne' or 'Eerstelijnsdienst'), which acts as a triage department to identify which complaints and requests merit further investigation and possible enforcement action. Such complaint or request may be filed by a natural or legal person (eg, a consumer rights organisation). At the risk of being found inadmissible, complaints and requests must fulfil certain procedural requirements. For example, they must be drafted in an official language of Belgium (ie, Dutch, French or German) and contain a brief description of the circumstances of the case. The Data Protection Authority has published electronic submission forms on its website to facilitate this process. The Frontline Service strives to handle admissible complaints and requests itself by proposing a mediation procedure to all parties involved. When mediation cannot be achieved, or when severe indications of data protection infringements exist, the Frontline Service will refer the case to the Dispute Resolution Chamber ('Chambre Contentieuse' or 'Geschillenkamer'). The procedure before the Dispute Resolution Chamber is more substantial and elaborate than the procedure before the Frontline Service. As the Dispute Resolution Chamber is a judicial body, proce-

dural rules and principles will have to be respected. Also, the Dispute Resolution Chamber at this point in the procedure may unilaterally still decide to dismiss the case without any further investigation or consequence.

Following a referral, the Dispute Resolution Chamber may request the Inspection Body ('Service d'Inspection' or 'Inspectiedienst') to take investigative measures. Such measures may include the identification, interrogation and written examination of individuals, on-site investigations, the accessing of IT systems and electronic data and copying of data found on such systems, seizing and/or sealing of goods or IT systems, and the identification of the user of an electronic communication service or means. All investigations are in principle confidential and the Inspection Body may request police assistance where required. When individuals are interrogated, similar due process rights apply compared to those in criminal investigations – the individual has the right to legal assistance, the right to obtain a copy of the interrogation report, and may request certain investigative action to be taken. To obtain access to private property (such as the individual's home) or to professional areas where an individual or entity exercises activity covered by professional privilege (such as a law office or doctor's practice), the Inspection Body must obtain the individual's permission or a search warrant. If the Inspection Body decides to seize or seal goods or IT systems, it can do so for a period of up to 72 hours, unless specific authorisation is obtained. Parties involved can file an appeal against any seizure or affixing of seals with the Dispute Resolution Chamber. All investigative measures give rise to a written report, which, along with any evidence found during the investigation, will serve as evidence in the administrative proceeding before the Dispute Resolution Chamber. To prevent imminent, serious and irreparable harm that may be caused by certain data processing activities, the Inspection Body can also impose preliminary measures, such as the suspension or limitation of ongoing data processing activities. Parties involved have the right to be heard prior to the imposition of any preliminary measures, and may also file an appeal against the decision imposing such measures with the Dispute Resolution Chamber.

Once the investigation is concluded, the Inspection Body may decide to refer the case to the Dispute Resolution Chamber where administrative proceedings on the merits will be initiated (unless the Dispute Resolution Chamber decides to dismiss the case, to propose mediation or to issue a warning). Where relevant, it may also decide to refer the case to competent criminal authorities in Belgium or to a supervisory authority of another EU Member State. As indicated above, where actual administrative proceedings on the merits are initiated, regular judicial safeguards and warranties kick in, such as the right of all parties involved to file written submissions and evidence, and the right to be heard. After conclusion of proceedings, the Dispute Resolution Chamber may decide to impose sanctions and corrective measures provided in the GDPR, including the imposition of penalties and administrative fines, the suspension of cross-border data transfers and the order to publish its decision on the website of the Belgian Data Protection Authority. All decisions imposing an administrative fine must be duly motivated (ie, by citing all reasons on which the decision to impose a fine was based). Administrative fines must be paid within 30 days after the day on which the decision was communicated. Parties involved may appeal decisions of the Dispute Resolution Chamber with the Commercial Court of Appeal ('Cour des Marchés' or 'Marktenhof') within 30 days after the day on which the decision was communicated. However, the decision of the Dispute Resolution Chamber will have executory force during any appeal proceedings.

The Data Protection Authority may also initiate enforcement action (including investigations) on its own initiative. This usually happens when the Data Protection Authority has heard about possible infringements of data protection law from other authorities or via the media.

Besides the administrative proceedings track, a plaintiff has the option to initiate criminal or civil proceedings in Belgium for infringement of his or her data protection rights. Criminal proceedings are initiated by an individual by criminal complaint filed with police authorities or by initiating action through the examining magistrate ('Juge d'Instruction' or 'Onderzoeksrechter'). Civil proceedings are typically initiated by writ of summons, and may exist in a claim for compensation or injunction procedure, which puts a (preliminary) stop to prima facie (seemingly) infringing data processing activities. In order to have legal standing before a civil court, the individual must demonstrate that harm was caused by the data protection infringement.

1.4 Multilateral and Subnational Issues

Belgium is a federal state with a civil law legal system, which means core legal principles are codified into a referable system that serves as the primary source of law. Unlike jurisdictions operating under the common-law system, these codified sources of law are applied and interpreted by judicial authorities, whose judgments and decisions do not have legislative force. The Belgian legal system is characterised by a hierarchy of legal norms and sources, in which legislation (national and regional laws and decrees) is considered more imperative than jurisprudence and legal doctrine. Such 'lower' sources from a hierarchical perspective cannot contradict higher-placed sources.

Historically, the Belgian Constitution was the highest legal source. However, a Supreme Court judgment of 1971 (Franco-Suisse Le Ski), placed international and European sources of law that apply to Belgian legal order (including EU regulations and directives) above the Constitution, making them

the highest legal source, preceding national laws, including the Constitution.

Belgium as a federal state is made up of different regions and communities that each have their own legislative powers, namely the Flemish, Walloon and Brussels-Capital Regions and the Flemish, French and German-speaking Communities. The governments of these regions and communities have the power to adopt legislation within the limits of the competence level attributed to them. Data protection as such is not recognised as a specific competence level, but clearly spills over into various competence levels attributed to the regions and communities. For instance, regions are competent to adopt legislation with respect to healthcare, and such legislation will contain provisions covering data protection principles to be respected by the healthcare sector. Region and community decrees have equivalent powers to laws adopted at federal level.

As indicated above, at the level of the Flemish Region and Community, a decree was adopted to establish a specific regulator to oversee data processing activities by the Flemish public authorities. The Flemish Government adopted a 'GDPR Decree' to bring existing Flemish legislation in line with the GDPR. The GDPR Decree does not include extensive substantive reform of existing Flemish legislation, but takes the opportunity to clarify the rules in light of the GDPR. As such, it establishes that individual rights can be limited when necessary in the context of an investigation on the basis of certain labour or social law requirements, and that the function of 'security consultant' (which is an internal role historically created to oversee information security) may be fulfilled by the organisation's data protection officer (DPO).

1.5 Major NGOs and Self-Regulatory Organisations

Belgium has a number of non-profit organisations that issue opinions on and may act on behalf of individuals to foster their data protection rights. Key non-profit organisations are the 'Liga voor Mensenrechten' (www.mensenrechten.be), a fundamental rights organisation, and 'Test-Aankoop' (www.test-aankoop.be), a consumer rights organisation. Belgium also has industry self-regulatory organisations, including the 'Jury voor Ethische Praktijken inzake Reclame' (www.jep.be, the 'JEP'), an organisation that regulates the advertising industry. JEP handles complaints and issues advice in relation to legal and ethical standards applicable to the advertising industry. It also issues relevant self-regulating codes of conduct.

As briefly indicated above, NGOs and SROs have legal standing to initiate administrative proceedings before the Belgian Data Protection Authority on behalf of an individual.

1.6 System Characteristics

The SA and DP Act include detailed descriptions of the administrative procedures to be followed by and before the Belgian Data Protection Authority, which go beyond the level of detail described in the GDPR. This suggests that data protection enforcement – as well as the associated rights of defence – will be taken seriously in the new regulatory regime. As briefly indicated above, investigative procedural rules appear to be inspired in part by Belgian criminal procedure and the procedure of descriptive seizure ('saisie-contrefaçon'), which is a procedure to gather evidence in IP infringement cases.

1.7 Key Developments

As is the case for the majority of EU Member States since the GDPR came into force, a number of key developments in data protection law have presented themselves in Belgium over the past year. Belgium has adopted two key legislative acts to govern data protection matters (supplementing the GDPR), namely the SA and DP Act. In addition, a new Camera Act was issued to govern the use of cameras for surveillance purposes. A new supervisory authority, the Data Protection Authority, was established by virtue of the SA Act. Since its creation, the Data Protection Authority has issued opinions and recommendations on the interpretation of Data Protection Impact Assessments (DPIAs) and the publication of a form that may be used for purposes of prior consultations following a DPIA, including a 'white' and 'black list'. The Data Protection Authority has also provided guidance on the requirements around data processing records (within the meaning of Article 30 of the GDPR) and the appointment of a DPO. Furthermore, the Data Protection Authority is in the process of updating thematic or industry-specific guidance in light of the GDPR and the new Belgian legislation, such as privacy in the employment area, privacy and direct marketing, and the impact of privacy on the use of biometrics.

To date, there has been no enforcement action on the basis of the GDPR or supplementing Belgian legislation. In February 2018, however, a first-instance judgment was rendered on the merits of the civil litigation against Facebook, which was initiated by the predecessor of the Data Protection Authority, the Privacy Commission, in 2015 on the basis of the previous Data Protection Act of 1992.

1.8 Significant Pending Changes, Hot Topics and Issues

As is the case for a number of EU supervisory authorities, the Belgian Data Protection Authority had to adjust to its new role and experienced staffing issues immediately after the new regime came into force. This could help explain why no major enforcement actions were taken in the first nine months after the GDPR became applicable. The Data Protection Authority has also indicated that, in terms of future data protection enforcement action, it will likely focus on

compliance in the insurance, banking and advertising industries initially. However, other industry sectors could also be scrutinised if the Data Protection Authority feels there is a need to do so. Lastly, and save unexpected setbacks, the e-Privacy Regulation is expected to be adopted sometime in the next 12 months. As with the GDPR, the e-Privacy Regulation will have direct effect in Belgian legal order and will not need implementation into national law (but might also leave room for national supplementing legislation).

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

As indicated above in **1.1 Laws**, and in addition to the GDPR, the Belgian data protection legislative framework is made up of two 'omnibus' laws – the SA Act and DP Act. These laws are sector-neutral and their scope of application mirror that of the GDPR, in that they apply to personal data processing activities that:

- take place in the context of an organisation's establishment in Belgium;
- relate to individuals in Belgium by an organisation that is not located in the EU when processing involves the targeting or monitoring of such individuals; and
- are performed by a controller established outside the EU where Belgian law applies by virtue of public international law.

The Belgian DP Act further specifies that, where a controller established outside the Belgian territory but within an EU Member State engages a processor established in Belgium, the laws of the EU Member State where the controller is established shall apply to the processor, provided that the processing is performed in that EU Member State.

The DP Act mainly adopts the principles of the GDPR, and only deviates from them in certain areas, such as children's consent and criminal data processing. Along with the majority of other EU Member States, Belgium has lowered the minimum age for children's consent to 13 years of age. Compared to the GDPR, the DP Act significantly broadens the scope for data processing related to criminal offences and convictions, allowing for such processing, for example, to manage legal disputes or with the individual's explicit written consent. Belgium also chose to implement the GDPR's provision allowing Member States to provide additional penalties applicable to GDPR infringements, and it expressly includes criminal sanctions for infringements of the DP Act. Such criminal sanctions mainly consist of criminal fines, which are, at a maximum of EUR240,000, significantly lower than the administrative fines that can be imposed under the GDPR.

The requirement to appoint a DPO is not expressly addressed in the Belgian DP Act or SA Act, but applies by virtue of the GDPR (which has direct effect in the Belgian legal system). The Belgian DP Act, however, has extended this requirement to certain processing activities that fall outside of the GDPR's scope of application, such as processing by intelligence agencies, the national Coordination Unit for Threat Assessment (CUTA), and processing by law-enforcement authorities. For such processing, the requirement to appoint a DPO is absolute (meaning that no specific conditions must be fulfilled in order for the requirement to apply). The DP Act provides that data subject rights, including the right of the individual to be adequately informed about the processing of his or her data, may be significantly curtailed when the data are processed to serve a public interest, for instance by Belgian intelligence services, the CUTA and police authorities.

The DP Act expressly establishes that personal data processed for archiving, scientific research and statistical purposes must be anonymised or pseudonymised directly after collection, and that re-identification should only take place where necessary to achieve these purposes, and subject to the advice of the DPO. The DP Act does not elaborate on the requirement to conduct DPIAs, but the Data Protection Authority has issued specific guidance in this regard, which specifies situations in which a DPIA is mandatory ('black list', eg, in the case of large-scale profiling activities) and cases where a DPIA must not be performed ('white list', eg, processing of payroll data).

In terms of redress, individuals have several options ranging from administrative to civil and even criminal redress. Administrative options (which may include mere complaint handling, mediation but also actual administrative proceedings) are led and handled by the Data Protection Authority. Whilst the individual can initiate action by filing a complaint or request, he or she does not have a significant level of control over the case and cannot claim compensation in the context of that procedure. A compensation claim needs to be filed with the civil courts, and the individual must be able to demonstrate that harm was suffered as a result of the infringement. Such a civil procedure can be initiated simultaneously with or after the administrative proceedings. As indicated above, certain infringements are punishable with criminal sanctions, such as non-compliance with the requirement to put in place appropriate data transfer mechanisms. For such infringements, criminal proceedings may be initiated (either by the public prosecutor or the individual himself). The concept of 'harm' is interpreted broadly as any detriment to an individual or his or her property, and can thus include pecuniary as well as moral harm (eg, reputational harm, embarrassment or 'loss of an opportunity'). There must, however, be a direct relationship between the harm suffered and the infringement, and the harm cannot be merely hypothetical. Historically, direct harm was a requirement for legal standing in legal proceedings. Recent-

ly, however, collective redress may be sought by non-profit organisations acting on behalf of a group of plaintiffs (see **2.5 Enforcement and Litigation** below).

2.2 Sectoral Issues

The concept of 'special category' or 'sensitive' personal data is not specifically defined in the law or regulatory guidance, causing the definition provided in the GDPR to apply. As such, it includes health data and data related to sex life or sexual orientation, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, genetic data and biometric data used for the purpose of uniquely identifying a natural person. Financial and communications data as such are not recognised as sensitive data.

The DP Act establishes that the processing of biometric, genetic and health-related data, which are all considered sensitive data, can only take place subject to specific safeguards. Pursuant to the Act, organisations processing these data must designate specific personnel authorised to access the data and identify their role in relation to the processing. A list with this information must be kept at the disposal of the Data Protection Authority. Such personnel must be bound by statutory or contractual confidentiality obligations. Under Belgian law, data related to criminal convictions and offences are not considered sensitive data. The legal bases for criminal data processing are broader compared to the GDPR and allow the processing of such data by natural and legal persons where necessary to manage their own disputes, by attorneys and other legal counsel in light of their client's defence, with the individual's consent or in case the data were made public by the individual, and where necessary for important reasons of public interest laid down by law or for scientific, historical or statistical purposes. Furthermore, the DP Act has lowered the age at which children can validly consent to the processing of their personal data, in the context of information society services, to 13 years.

The Belgian Data Protection Authority issued a recommendation on the use of cookies on 4 February 2015 ('Cookie Recommendation'), which sets out cookie recommendations and good practices for website owners, publishers, operators and advertisers. It clearly distinguishes essential from non-essential cookies and recommends that website owners include a cookie policy and banner.

In 2016, the two largest telecom companies in Belgium, providing mobile, landline and internet telecommunication, as well as digital TV services, decided to show users of their digital TV services targeted advertisements during commercial breaks. Users would be able to select privacy settings, allowing the advertisements to be categorised from 'significantly targeted' to 'little targeting,' depending on the level of personalisation following their user preferences. Significant targeting would, for instance, show advertisements based on the user's basic personal data (eg, name and invoicing address) as well as on his or her digital TV viewing habits and internet browsing behaviour. This decision was scrutinised by the Belgian Data Protection Authority (then the Privacy Commission) in 2017, which eventually decided to allow it, provided that the telecom companies would sufficiently inform existing users of this practice, and obtain opt-in consent from any new users/customers.

2.3 Online Marketing

Belgian law imposes specific restrictions on sending unsolicited marketing communications to individuals. The Belgian Code of Economic Law (CEL) and related legislation (such as the Belgian Royal Decree of 4 April 2003 on the regulation of electronic marketing communications) set out different restrictions per means of communication. For sending of electronic marketing messages (including email, SMS, MMS, voicemail and other types of communication transferred through electronic means that can be stored on or retrieved through a device), prior opt-in consent must be sought from the recipient. The Belgian Royal Decree of 4 April 2003 provides for exceptions to this principle of prior opt-in, namely when an organisation is able to rely on the so-called 'soft opt-in' exemption, or when generic business addresses are used. Under the soft opt-in exemption, there is no need to obtain opt-in consent from the individual where contact details were obtained in the context of a previous commercial transaction, the communication relates to similar goods or services offered by the same organisation, and the individual is given the opportunity to opt out from receiving (further) marketing communications. To strengthen and implement the opt-out right, the CEL sets forth that the service provider sending the marketing must:

- provide clear and understandable information on the right to opt-out; and
- identify and provide for an efficient way for individuals to exercise this right electronically and free from charge.

Similarly, if marketing messages are sent to non-personal corporate email addresses (eg, info@company.com) and are not targeted to a particular individual at that entity, the sender of the message does not need to obtain opt-in consent as long as it offers the recipient the right to opt-out in each marketing communication. Apart from this distinction, the Belgian rules on unsolicited marketing communications apply equally to communications sent to consumers and business alike (ie, independent from whether communications are sent in a B2C or B2B context). Lastly, no so-called 'Robinson Lists,' which require organisations to respect previously registered opt-outs by individuals (see below) are maintained for electronic marketing communications in Belgium.

The use of telemarketing via automated calling and marketing via facsimile is subject to a prior opt-in requirement, and no specific exemptions apply. Once opt-in is obtained from

the recipient, the latter must still be granted the right to opt-out at any time at no cost. The use of telemarketing via non-automated (ie, voice-to-voice) calls, however, is currently still permitted on the basis of an opt-out system. This essentially means that the recipient does not need to give prior opt-in consent, but must be merely provided with the option to refuse telemarketing at all times and at no cost. To facilitate the opt-out system, a 'Robinson List' (entitled 'Do-Not-Call-Me,' at https://www.dncm.be/nl/) was put in place at national level where Belgian recipients can register to refuse calls from telemarketers. Prior to launching a telemarketing campaign, telemarketers must check all intended recipients against this list in order to identify who has expressed an opt-out via the list. This opt-out system for voice-to-voice telemarketing was recently scrutinised by the Belgian Parliament, where it suggested to amend the law and introduce an opt-in system for telemarketing. However, this legislative proposal was not pursued, and to date the opt-out system remains in place. The soft opt-in and generic email address exemptions do not apply to voice-to-voice telemarketing.

In addition to the above, all direct marketing through electronic mail must adhere to more general requirements pursuant to CEL, including:

- it must contain the term/designation 'advertising' in a clearly legible, visible and transparent manner (unless it is clear from other indicators that the communication contains advertising);
- it must clearly identify the legal entity on whose behalf the advertising is being sent; and
- it must clearly identify any offers aimed at incentivising purchase (eg, notifications of price reductions and related offers) and conditions that apply to such offers.

Behavioural advertising is governed by a multitude of legal principles and laws. The 'profiling' activity that precedes and permits targeted or 'behavioural' advertising is restricted by data protection and e-privacy principles. The GDPR, for example, defines 'profiling' as data processing to evaluate an individual's behaviour or other aspects (eg, to analyse or predict purchasing behaviour). Whilst profiling that does not result in automated decision-making, can – in theory – be legitimised on the basis of the different legal bases provided in the GDPR (ie, consent, contract performance, compliance with a legal obligation, and legitimate interests), behavioural advertising that results in automated decision-making in principle requires the individual's explicit consent.

Profiling is often performed using 'tracking' cookies that assess the individual's behaviour across different websites. They often provide invaluable insight into the individual's purchase behaviour and other preferences or characteristics. The use of such tracking cookies is subject to e-privacy requirements that in Belgium are implemented in the Electronic Communications Act and that in essence require prior opt-in consent from the individual to use such cookies (eg, by implementing a cookie banner). Finally, as discussed above, the sending of direct marketing communications may also be subject to specific conditions and restrictions, such as the individual's prior opt-in consent. It remains to be seen whether or not these requirements will change substantially once the new EU e-Privacy Regulation is in place.

Belgian law does not impose specific requirements or conditions for location-based advertising. In general, the same principles as for behavioural advertising apply.

2.4 Workplace Privacy

From a data protection law perspective, both the GDPR and the DP Act apply to the processing of personal data in an employment context. No sector-specific privacy laws exist at this point, but several CLAs have been adopted to regulate privacy at the workplace, at least to some extent. There are currently CLAs in place covering topics such as camera surveillance, e-monitoring of employees, theft prevention and exit control for employees, as well as medical testing of employees and job applicants.

These laws and CLAs are based on the general principle that a balance must be found between the employee's right to privacy and the employer's legitimate interest to exercise a certain level of control over individuals who are in an employment relationship with the employer. A justifiable level of control by the employer assumes, for instance, that the employer should be able to monitor employee behaviour to detect fraud (as further described below). Any limitation of the right to privacy must be justified by a valid legal basis, serve a legitimate purpose, and be proportionate and subject to prior information and transparency obligations.

It is important to emphasise the role of collective bargaining in shaping the rules on workplace privacy, which has resulted in a regime that heavily protects the interests of employees. In addition, employment laws may be adopted at national, communal or regional level, making the legislative landscape highly complex.

Employers may monitor the use of electronic online communications (eg, email, SMS, MMS and internet use, collectively known as 'e-monitoring') by employees in accordance with the conditions set out in CLA No 81 on e-monitoring. This CLA sets out the general principles of privacy and data protection, and establishes that an employer may perform such e-monitoring for purposes including:

- the prevention of wrongful or defamatory acts or acts that violate general morals or principles of human dignity;
- the protection of confidential economic, commercial and financial interests of the organisation and the combat of acts that infringe these interests;

- the preservation of the security and/or functioning of the organisation's IT systems, including the monitoring of related costs and the protection of company premises; and
- good-faith compliance with company policies and procedures governing the use of online technology.

As long as one of these purposes are fulfilled, the employer does not need to obtain employee consent (which would be problematic in any event given the employer–employee relationship). Specific procedural rules must be respected when monitoring employees, including the provision of prior information to all employees involved and the implementation of a two-step procedure where personal data relating to identified employees are only processed in a second stage.

In 2012, the Data Protection Authority (then Privacy Commission) issued guidance on e-monitoring in which it formulated several recommendations. In essence, CLA no 81 and the Data Protection Authority share the opinion that both professional and personal communications may be monitored by the employer (whereby the latter are subject to more stringent requirements). To prevent personal communication from unlawful monitoring, they recommend either marking personal emails as 'personal' or storing them in a personal folder. In addition, the organisation could appoint a trusted individual who, acting as a human 'filter,' could be responsible for the manual review of an employee's emails to ensure that the employer does not accidentally access personal emails.

With the exception of a limited number of specific situations, there is an express statutory prohibition to record or listen to an employee's telephone conversations. However, the employee's telephone use as such (eg, the time and duration of a phone call) can be monitored as long as the organisation has a legitimate interest to do so and has adequately informed the employee.

Employee representative bodies, such as works councils and labour unions, must be informed prior to the implementation of employee monitoring systems and should be able to evaluate the system regularly.

Following the Data Protection Authority's recommendation on the implementation of whistle-blowing schemes of 29 November 2006 ('Whistle-blowing Recommendation'), personal data processing through whistle-blowing hotlines in Belgium can be justified on the basis of a legal or regulatory requirement to process data through a hotline or, in the absence of such a requirement, on the basis of the organisation's legitimate interests. Such a legal or regulatory requirement can only be relied on where it is laid down in Belgian law or regulations. However, foreign law requirements, such as obligations under the Sarbanes-Oxley Act, can be taken into account for purposes of establishing a legitimate interests ground. Whistle-blowing reporting in Belgium is not limited in scope, but the Data Protection Authority recommends that hotlines should only be used for reporting serious issues (eg, criminal law violations) that cannot be reported using the organisation's regular internal reporting channels (eg, by reaching out to a direct superior). Organisations are expected to provide all employees with an information notice about the hotline and how it affects their personal data. In addition, there should also be a separate standard operating procedure that outlines how personal data collected via hotline reporting should be handled and protected.

Anonymous hotline reports (where the individual filing the report chooses to remain unidentified) are not expressly prohibited, but should be discouraged. The Belgian Data Protection Authority shares the view of the European Data Protection Board (previously Working Party 29) on this point, and considers that anonymous reporting should be the exception to the rule and that organisations must clearly communicate that they will protect the identity of the individual submitting the report.

Where justified, the employer may install a geolocation device in an employee's vehicle. This will, for instance, be the case where it is necessary for the employee's own safety (such as in the case of security services) or when it is necessary to optimise a service (such as a taxi service). Systematic geolocation is in principle not allowed, save in the case of, for instance, the transport of dangerous substances.

2.5 Enforcement and Litigation

No specific standard of proof applies to Belgian civil or administrative proceedings, but there is a general hierarchy of evidence that must be respected. Generally, a confession is given more weight than regular written evidence, which is given more weight than testimonies and suspicions.

The enforcement penalties that may be imposed in the context of an administrative procedure before the Data Protection Authority mainly reflect the GDPR's corrective measures (and may consist of administrative fines consisting of a maximum of EUR20 million or 4% of annual worldwide turnover, the issuance of warnings and reprimands and certain injunctive powers such as the order to suspend data flows). If the data protection violation constitutes a criminal offence in the eyes of the Data Protection Authority, it can choose to transfer the case to the public prosecutor for possible criminal prosecution. Criminal sanctions may include criminal fines of up to EUR240,000 and imprisonment of up to six months.

Since 2015, the Belgian Data Protection Authority has been involved in civil litigation brought against Facebook Inc and its Belgian and Irish subsidiary ('Facebook') before the Brussels Courts. The Data Protection Authority initi-

ated enforcement action against Facebook for the alleged unlawful tracking of online activities of Belgian individuals with and without a Facebook account. The case was initiated in summary proceedings, mostly aimed at non-Facebook account-holders, and subsequently proceedings on the merits, which covered both account and non-account holders. Facebook won the summary proceedings on appeal in June 2016 on procedural grounds, namely that the Brussels Court had no jurisdiction over Facebook Inc and its Irish subsidiary, which are established outside Belgium. The court also found that urgency – a prerequisite to initiate summary proceedings in Belgium – was not demonstrated, thereby also dismissing claims against Facebook Belgium. The Data Protection Authority, however, won the merits proceedings in first instance in February 2018 and the court ordered Facebook to stop the online tracking of internet users on Belgian territory through the use of tracking cookies and related technology without obtaining the user's informed consent and without offering an opt-out mechanism. In this case, the court used the territoriality principle in public international law (which declares a national court competent over conduct occurring on national territory) to assume jurisdiction over the two non-Belgian Facebook entities. The Belgian court ruled that material non-compliance with its judgment would result in penalty payments of EUR250,000 per day of non-compliance, capped at EUR100 million. Facebook has appealed the first instance judgment of the Brussels court and appeal proceedings are still pending. Pleadings are scheduled for 27 and 28 March 2019, and an appeals judgment is expected in mid-2019.

As indicated above, no legal standards of proof apply to Belgian civil litigation. Claimants must in principle fulfil the 'personal interest' or legal standing requirement to validly initiate legal proceedings in Belgium. In 2014, however, Belgium slightly deviated from this principle with the adoption of the Class Action Act, which allows groups of consumers to initiate collective redress by mandating a non-profit organisation or public body. The Class Action Act requires such collective action to be directed at corporate entities and focused on consumer rights allegations. The DP Act now also allows for one or a group of individuals to mandate non-profit organisations or other body to file complaints and to act on their behalf in consequent proceedings. In order for such 'class action' type suit to be admissible, the organisation will have to be adequately recognised in Belgium, have legal personality and a public interest mission, and be active in data protection matters for at least three years.

No high-profile or prominent private litigation has been initiated to date.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

As indicated above, Belgium has implemented EU Law Enforcement Directive 2016/680 (LED) in the DP Act, which sets out general principles of data processing for law enforcement purposes, including public security and intelligence services. The Belgian Criminal Procedural Law Code (CPC) permits accessing of personal data by several competent authorities when this is necessary in light of the prevention, investigation and prosecution of criminal offences and the execution of sanctions. In Belgium, evidence (and personal data) can be collected in two types of criminal investigation phases – the preliminary investigation ('opsporingsonderzoek') and judicial investigation ('gerechtelijk onderzoek'). The former is led by a public prosecutor ('Procureur des Konings') and the latter by a specifically appointed judge who manages the investigation phase and has more far-reaching powers (the instruction judge or 'Onderzoeksrechter'). Only the public prosecutor and the instruction judge have the power to determine which measures are necessary and appropriate to adequately investigate an offence. In 2003, both the public prosecutor and instruction judge were given more far-reaching investigative powers that have a clear impact on privacy following the adoption of the Law of 6 January 2003 on Special Investigative Acts (SIA). On the basis of this Act and when there are sufficient indications of serious crimes, the public prosecutor can intercept and seize regular mail, and the instruction judge can authorise covert surveillance of private homes and wiretapping. Since 2017, these measures have been expanded further and include the power for the public prosecutor to authorise police authorities to infiltrate via the internet and collect relevant data by covertly reaching out to a suspect. Police authorities can also access data in the context of crime investigation and prevention, but their powers are more limited. They may, for instance, decide to install and use CCTV imaging in certain areas and perform body searches and identity checks.

3.2 Laws and Standards for Access to Data for National Security Purposes

Belgian criminal procedural law includes several more specific laws providing for far-reaching government access when this is necessary in the context of the fight against terrorism, intelligence or other national security purposes, and relevant investigative measures and powers have been expanded further following a substantive legislative reform triggered by the terrorist attacks in Paris and Brussels in 2015 and 2016. In general, the ability to investigate terrorist activities through the collection of relevant data has been expanded, but safeguards still exist by means of the 'filter' position of the instruction judge (who has the authority to order far-reaching investigative measures) and by requiring sufficient indications of such activities. More specifically, the reform

(named the 'Terro I,' 'Terro II' and 'Terro III' laws) included the creation of a dynamic database that contains all relevant information on persons qualified as 'foreign terrorist fighters' collected by national intelligence services. The database will be accessible by all relevant Belgian authorities, including the national security agency, public prosecutors, and the Coordination Unit for Threat Assessment (CUTA) which is a unit responsible for evaluating terrorist and extremist threats in Belgium. In addition, the modalities of searches for private homes were modified to allow searches during the night, if there are sufficient indications of terrorist activities.

3.3 Invoking a Foreign Government

There is currently no explicit basis in Belgian law for private companies to collect and/or directly transfer personal data from Belgium in response to a request from foreign official authorities. For foreign authorities to access personal data in Belgium a request must be made under a (bilateral) Mutual Legal Assistance Treaty or 'MLAT' (such as the treaty between Belgium and the US on mutual legal assistance in criminal matters). This means data will be transferred between the official law enforcement authorities of both countries (and not from a private Belgian company to a US official authority). For data transfers within the European Economic Area (EEA), similar legal frameworks have been put in place, such as the EU Framework Decision of 18 December 2006 on the expedited and easy exchange of information between law enforcement authorities (also known as the 'Swedish Initiative'). This decision has been implemented into Belgian law and facilitates data-sharing between Belgian and non-Belgian law enforcement authorities.

Apart from establishing a legal basis for the data transfer (being a processing activity in itself), a transfer to a recipient in a third country outside the EEA can only take place when it meets the conditions of Chapter V of the GDPR (eg, if the data protection regime in the third country has been found to be adequate by the European Commission, or if a data transfer mechanism has been put in place). According to Article 48 of the GDPR, decisions from third-country authorities or governments are not in themselves sufficient to allow data transfers to third countries. This means that, when an international agreement such as an MLAT is in place, EU companies should generally reject direct requests from foreign authorities and refer the requesting authority to the existing MLAT. However, guidance issued by the EDPB appears to provide more flexibility, by allowing data transfers in response to a foreign authority access request where this is necessary in the context of the defence of legal claims (eg, for foreign investigations or pre-trail discovery).

Noteworthy is that in March 2018, the US CLOUD Act was adopted, allowing US law enforcement agencies to request direct access to data from private companies outside the US. This in essence relieves US authorities from the obligation to obtain the data through a local warrant or by initiating procedures on the basis of a MLAT. In the wake of the US CLOUD Act, the European Commission has proposed a similar legislative package. The European legislative proposal of April 2018 is composed of a draft Regulation and Directive, allowing EU judicial and law-enforcement authorities to obtain direct access to data under an EU service-provider's control that are stored inside or outside the EU. The European Commission has indicated that this legislative package is one of its top legislative priorities for 2019.

3.4 Key Privacy Issues, Conflicts and Public Debates

Please refer to **3.3 Invoking a Foreign Government Request** above.

4. International Considerations

4.1 Restrictions on International Data Issues

As long as the general principles of the GDPR are respected – eg, legal basis for the transfer, compatibility with original processing and sufficient transparency around the transfer – and the requirements in Chapter V of the GDPR are met, there are no additional restrictions to international data transfers outside of Belgium.

4.2 Mechanisms That Apply to International Data Transfers

Belgian data protection law supports all data-transfer mechanisms provided in the GDPR, including the use of standard contractual clauses, binding corporate rules, and the EU-U.S. Privacy Shield and accepts that data may be transferred on the basis of a derogation such as the individual's explicit consent. In principle, the individual concerned must be informed of the data transfer prior to the actual transfer, but the Belgian DP Act provides for exceptions in the area of law enforcement and intelligence services.

4.3 Government Notifications and Approvals

No prior governmental or regulatory authorisation or notification is required to transfer data outside Belgium. However, the Belgian Data Protection Authority does support and commits to contributing actively to the system of approved codes of conduct and certification mechanisms as mechanisms for the international transfer of data. In addition, the Belgian Data Protection Authority will need to be informed of data transfers outside the EEA that take place on the basis of an organisation's compelling legitimate interests.

4.4 Data Localisation Requirements

There are no data localisation requirements under Belgian law. Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data, which is expected to enter into force in mid-2019.

4.5 Sharing Technical Details
Organisations are not required to communicate their use of specific technical equipment or software to the government or Belgian Data Protection Authority.

4.6 Limitations and Considerations
Please refer to **3.3 Invoking a Foreign Government Request** above.

4.7 "Blocking" Statutes
There is one blocking statute that applies in Belgium in the context of fair competition in the Belgian sea and air transport sectors. The Belgian Act on the Regulation of Sea and Air Transport, as amended and implemented in the Belgian CEL, and the corresponding Royal Decree, provide that Belgian individuals and organisations operating in the sea and air transport sector are prohibited from complying with foreign measures or decisions when these relate to Belgian competition, abuse of dominance, or unfair commercial practices regulations. This prohibition of non-compliance covers any act that directly or indirectly, includes the provision of information or statements and the communication of documents.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law
The use of drones has been specifically regulated in Belgium since April 2016. The Royal Decree of 10 April 2016 on the use of drones (the 'Drone Decree') stipulates that recreational use of a drone is permitted indoors and outdoors in privately owned places with the owner's consent. Other conditions must also be fulfilled, such as the restriction that the drone should not pass an altitude of ten metres above ground level and should stay within the pilot's field of vision. Other use will be qualified as 'non-recreational' or 'professional' drone use, and has to comply with more stringent requirements and obtain a drone certification or specific authorisation (which requires the passing of an exam that also tests relevant data protection law knowledge). Drones can collect a wide set of personal data, for instance through the use of a surveillance camera or through sound recordings. For both recreational and professional drone use, the pilot must respect Belgian data protection law and if the drone is equipped with a camera, the Belgian Camera Act applies. In the absence of specific data-protection legislation for drones, the Data Protection Authority has issued guidance in this context. To comply with the general transparency principle, for instance, the Data Protection Authority recommends that the drone be painted in a specific colour to enhance visibility, that the company's logo or colours be visible on the drone, and/or to announce the use of drones and related details in the media prior to using them.

There is no specific legislation governing the use of biometric data, but the new DP Act provides for additional restrictions or modalities when biometric data are processed. In such a case, the data controller is required to keep a list of persons who are authorised to access the data and their role in relation to the data processing. The list must be kept at the Data Protection Authority's disposal at all times. In addition, the controller must ensure that these persons are bound by strict confidentiality requirements.

Belgium is investing heavily in new technologies involving autonomous decision-making and the Internet of Things (IoT). In May 2018, the Royal Decree on the Use of Public Roads (the 'Traffic Regulations') was amended to allow testing of autonomous vehicles on public roads (namely by preventing full application of the Traffic Regulations to these vehicles, offering more scope for 'trial and error').

6. Cybersecurity and Data Breaches

6.1 Key Laws and Regulators
The Belgian DP Act does not contain data breach notification provisions applicable to general processing operations, but the GDPR applies in this regard by virtue of its direct effect. For a number of specific processing operations that are excluded from the GDPR's scope of application – namely data processing by national law enforcement authorities, intelligence services, the CUTA and the Passenger Information Unit – the DP Act imposes data breach notification requirements that are virtually identical to the ones included in the GDPR, but these entities (with the exception of CUTA) need to report data breaches to a specific regulator named Committee I ('Vast Comité I'). In addition, providers of publicly available electronic communications services are, under certain conditions, required to notify a data breach to the Data Protection Authority under the Electronic Communications Act within 24 hours after detection of the breach.

As indicated above, the Flemish Supervisory Commission has exclusive competence to receive and handle data breach notifications from Flemish public authorities. The GDPR requirements and thresholds apply, and notifications can be made through completion of an online form that is available on the Flemish Supervisory Commission's website.

In addition, Belgium is in the process of implementing the EU Network and Information Systems Directive 2016/1148 (the 'NIS Directive'), which establishes technical and organisational measures (such as breach-notification requirements) for operators of essential services (or 'critical infrastructure,' such as transport, drinking water and public health) and digital service-providers to handle and prevent incidents. The current draft of the law implementing the NIS Directive of 12 November 2018 (the 'Draft NIS Act') applies to operators of essential services that have an establishment

and provide an essential service in Belgium, and to digital service-providers whose main establishment is in Belgium. Operators of essential services are required to report incidents with a significant impact on the continuity of the service to three authorities simultaneously – the national Computer Security Incident Response Team (CSIRT), the sectoral government or sectoral CSIRT, and the authority co-ordinating the identification of essential services operators (which is still to be appointed by Royal Decree). The National Bank of Belgium is competent to receive reports of incidents arising in the financial sector. The European Union Agency for Network and Information Security (ENISA) will be granted an advisory role and Belgian authorities will co-operate and co-ordinate with ENISA at regular intervals.

6.2 Key Frameworks

There are no mandatory security standards that companies must adhere to in order to secure personal data. The Belgian Data Protection Authority does recommend to strive towards adherence to the information security guidelines of the Organisation of Economic Co-operation and Development (OECD) as a good practice.

6.3 Legal Requirements

As indicated above, the DP Act does not provide for specific security requirements or mandatory information security standards. The Data Protection Authority's Recommendation on Security Measures for the Prevention of Data Breaches of 21 January 2013 (which is currently under revision following entry into application of the GDPR) does recommend companies to have in place an information security policy and an incident response plan to prevent and handle incidents adequately. As a best practice, companies should also ensure that these policies are followed by their vendors. The Data Protection Authority also recommends implementing physical and technical access restriction measures (eg, to maintain lists of persons authorised to access and process certain data and install a logging system to keep track of access) and put in place adequate network security measures. In addition, the company should conduct regular risk assessments and audits to ensure security measures are still effective and meet state-of-the-art technology.

Sidley Austin LLP

NEO Building Rue Montoyer 51
Montoyerstraat
B-1000 Brussels

Tel: +32 2 504 6400
Fax: +32 2 504 6401
Email: wnauwelaerts@sidley.com
Web: www.sidley.com

There is no formal requirement to appoint a Chief Information Security Officer (CISO), but certain (sector-specific) Belgian laws require the appointment of a security consultant ('veiligheidsconsulent') for certain sectors such as hospitals and social security organisations. Security consultants have an advisory and compliance role in information security, and often lead the information security team. The role of security consultant could in practice also be fulfilled by the Data Protection Officer as provided in the GDPR. However, the role of CISO is not equivalent to the role of Data Protection Officer (DPO) under the GDPR, given the CISO's main role is to oversee information security, while the DPO's focus remains on data-protection compliance.

6.4 Key Affirmative Security Requirements

The Belgian Centre for Cyber Security (the appointed federal CSIRT) has adopted a Cyber Emergency Response Plan (the 'Plan') to combat major cyber-incidents on critical infrastructure. The Plan helps to formulate an appropriate response depending on the impact of the incident, and provides for co-ordination between several Belgian services to mitigate incidents as quickly as possible. In addition, the Centre has implemented an 'early-warning system' that is a shared automated platform that allows proactive sharing of information on incidents and threat among critical infrastructure. The Centre has also published a cyber-guide and cybersecurity kit to raise awareness in cybersecurity for SMEs and other organisations.

In December 2018, the EU institutions reached a political agreement on the EU Cybersecurity Act, aimed at strengthening the EU's and Member States' ability to tackle incidents and boost cybersecurity. Once formally adopted, the Act will put in place a harmonised framework for EU cybersecurity certificates for ICT products, processes and services that will be valid throughout the EU (and resolve the current patchy certification mechanisms that mainly rely on the ISO standards). Certification will require the implementation of the security by design principle into ICT products and services, which will be validated by independent and accredited bodies against a defined set of criteria and after which certification may be issued. The ultimate purpose of the certification mechanism is to help increase effective protection against data breaches.

6.5 Data Breach Reporting and Notification

Please refer to **6.1 Cybersecurity and Data Breaches**: **Key Laws and Regulators** above.

6.6 Cyberthreat Information Sharing Arrangements

The EU Cybersecurity Act provides for the facilitation of sectoral Information Sharing and Analysis Centres (ISACs) where cyber intelligence and knowledge may be exchanged between the public and private sector (in particular for criti-

cal infrastructure-providers). Belgian law does not contain more specific provisions in this respect.

6.7 Significant Cybersecurity, Data Breach Regulatory Enforcement and Litigation

No high-profile or prominent data-breach enforcement or litigation has been initiated to date.