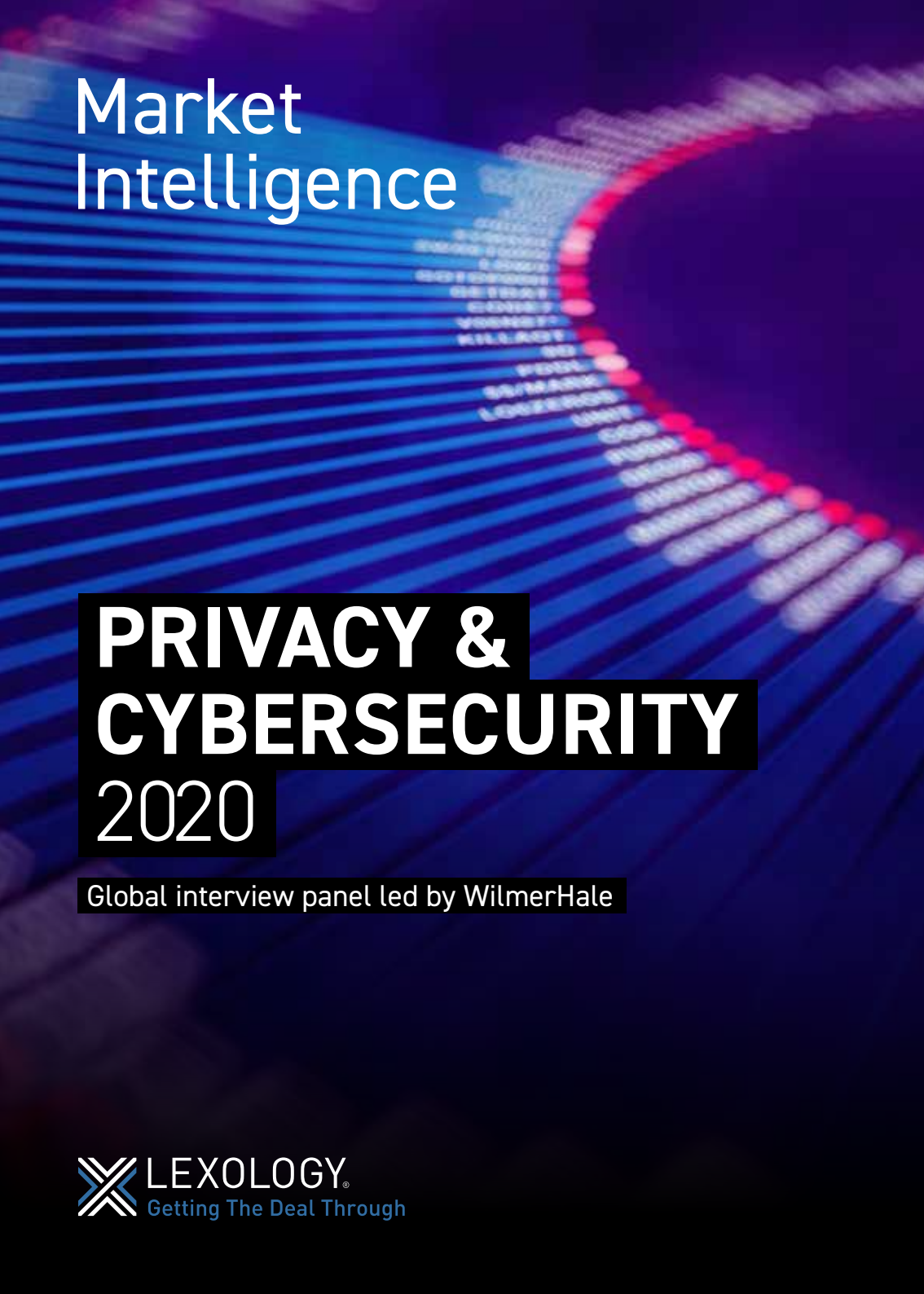


Market Intelligence

PRIVACY & CYBERSECURITY 2020

Global interview panel led by WilmerHale

LEXOLOGY®
Getting The Deal Through

LEXOLOGY
Getting The Deal Through

Publisher
Edward Costelloe
edward.costelloe@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Business development manager
Dan Brennan
dan.brennan@gettingthedealthrough.com

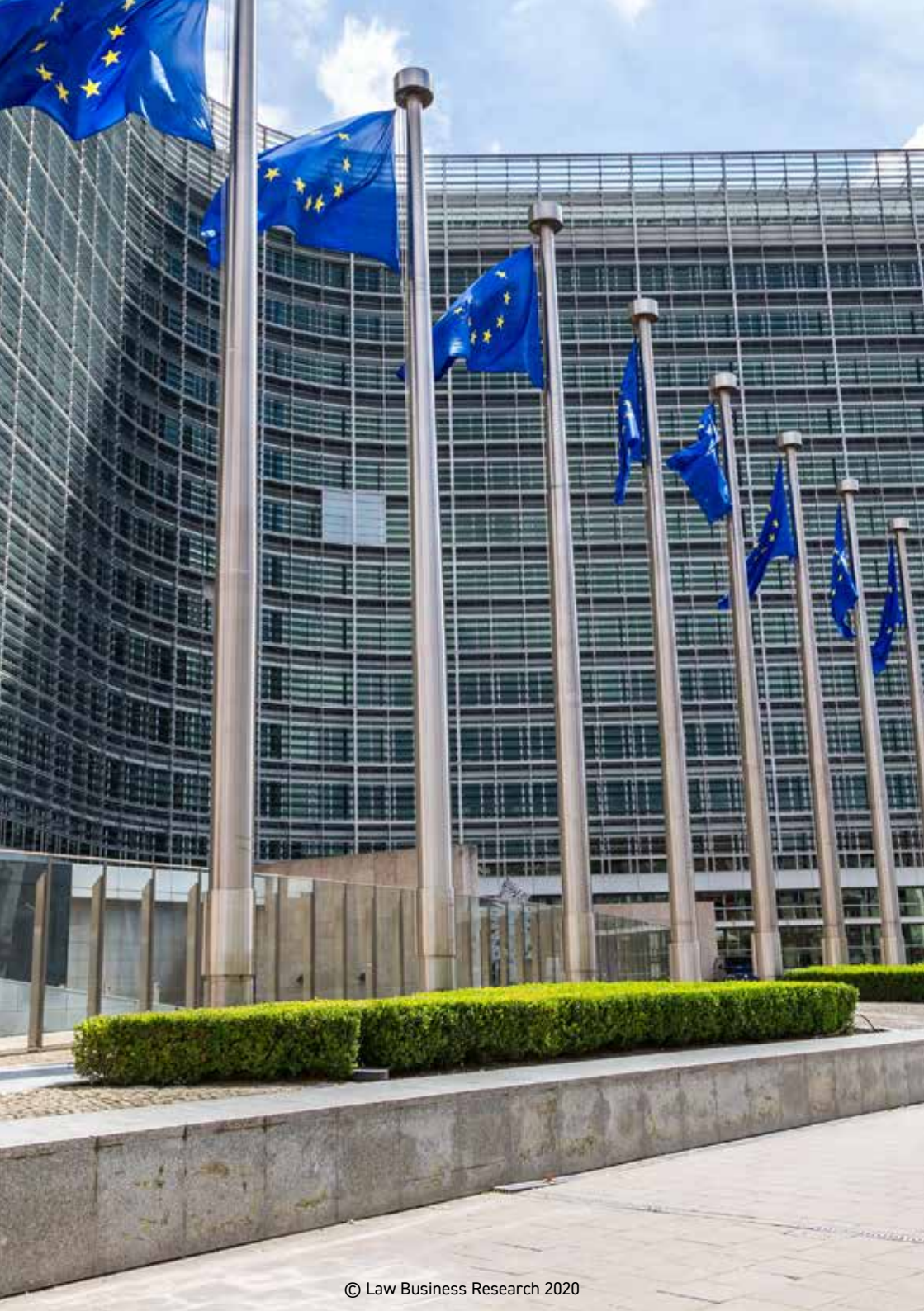
Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

Cover photo: shutterstock.com/g/handmadefont

ISBN: 978-1-83862-419-4

Printed and distributed by Encompass Print Solutions

Privacy & Cybersecurity 2020



The EU and Belgium

Christian Duvernoy, Anne Vallery and Itsiq Benizri are members of WilmerHale's regulatory and government affairs department, resident in the Brussels office.

Christian heads the office and focuses on the application of European Union (EU) competition law and regulation to sectors including IT and IP, financial services and other network and manufacturing industries. He regularly counsels on e-commerce and data protection compliance.

Anne has broad experience in EU and Belgian electronic communications regulation, data protection, cybersecurity and competition law. Her recent work includes advice to internet-based communications services and internet-of-things service providers on compliance worldwide, as well as successful regulatory appeals before Belgian courts.

Itsiq focuses on data protection and cybersecurity, in addition to electronic communications, e-commerce and competition law. He has experience in a broad set of sectors, including IT and cloud computing, communications, banking, energy, transport, gaming, pharma, sports and media. Itsiq is qualified as a certified information privacy professional (CIPP/E) by the International Association of Privacy Professionals and is a member of this association.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

The last time we talked was in mid-2018, so we obviously have a lot to discuss to cover the key regulatory developments over the past two years concerning cybersecurity standards. We first briefly recall the role that cybersecurity regulation plays in the EU and Belgium and how the legislative architecture for cybersecurity is constructed. We then summarise general cybersecurity developments in the EU and in Belgium in 2019–2020 before we move on to a description of more specific concerns and issues that have arisen.

Cybersecurity has relatively recently taken on key importance in the EU and in Belgium, given the vital role that digital networks and information technology systems and services play in society nowadays. However, the protection of personal data, which is also relevant for cybersecurity, has been a concern for more than 25 years in the EU and in Belgium and a fundamental human right for more than 10 years. For that reason, we discuss both technical cybersecurity, more narrowly understood, as well as data protection, which is part of a broader understanding of cybersecurity.

Since 2018, cybersecurity has been addressed at EU level through a number of regulations and directives that have the overall objective of promoting the single internal market in terms of an effective cybersecurity space within the EU. Data protection law includes cybersecurity requirements, such as the obligation to keep personal data secure and transfer it only if it is adequately protected. In addition, cybersecurity laws apply to critical infrastructure and specific sectors, even if personal data is not at issue. EU rules in some cases harmonise national rules, and in other cases provide an overlay on top of them, enabling companies to take a common approach to cybersecurity. Each EU member state is responsible for operational application and enforcement of the EU cybersecurity requirements and for how it organises the public authorities responsible for these tasks. As far as substance is concerned, EU cybersecurity instruments as well as the General Data Protection Regulation (GDPR) impose far-reaching requirements.

In 2019 and 2020, we observed several general developments that affect all key EU cybersecurity requirements. On the GDPR side, this includes the slow and sometimes controversial use of coordination mechanisms between the national data protection authorities (DPAs). Developments also include the European Commission's growing effort to recognise non-EU countries as offering adequate protection of personal data, including in terms of cybersecurity, and just as we go to press, the European Court of Justice (ECJ) has considerably limited the possibilities to transfer personal data from the EU to the US since it has ruled that the Privacy


Christian Duvernoy


Anne Vallery


Itsiq Benizri

"Cybersecurity has relatively recently taken on key importance in the EU and in Belgium."

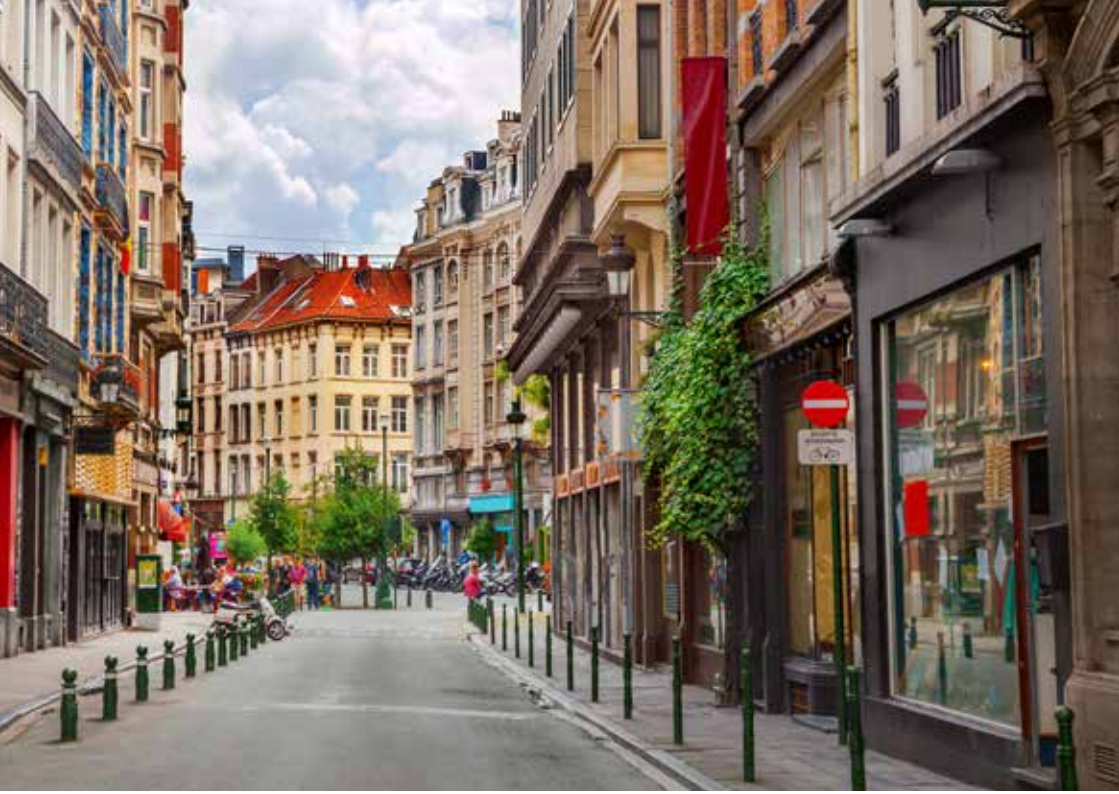


Photo: shutterstock.com/g/adisa

Shield is incompatible with EU law and has largely limited the possibilities for the effective use of standard contractual clauses (SCCs) for such transfers. During this period, Belgium transposed the Directive on security of network and information systems (NISD) and drew up a list of the operators of essential services (OES) that are established on its territory. In parallel, the European Commission (EC) has already started reviewing NISD with a view to amending the Directive. Electronic communications have seen a major regulatory update with the adoption of the European Electronic Communications Code (EECC) in late 2018. Member states are required to transpose the EECC into national law by the end of 2020. The EU's Cybersecurity Act, revising the rules governing the EU Agency for Cybersecurity (ENISA) and creating a cybersecurity certification framework, was adopted in April 2019. While the prospects for adoption of an EU-level ePrivacy Regulation have worsened, the latest amended proposal that was published is less relevant from a cybersecurity perspective.

We also observed more specific concerns and debates regarding cybersecurity, in particular in relation to new global challenges and the deployment of new technologies. Specific cybersecurity developments include guidance by DPAs to address

the increased cybersecurity risks raised by the covid-19 crisis and heated debate regarding the development of contact-tracing apps to fight the spread of the virus and support deconfinement measures. Much attention has also been paid to the cybersecurity risks that the deployment of 5G networks, artificial intelligence (AI) and connected vehicles could bring. Finally, full application of the new Payment Services Directive (PSD2) means stronger cybersecurity requirements for online payment services.

First, it is probably best to expand on the general cybersecurity developments starting with the GDPR, given the key role that it plays in the EU cybersecurity regulatory framework and the source of inspiration that it represents for many lawmakers around the world. The GDPR impacts all private and public-sector entities. There are broad exceptions to the GDPR, so that it does not apply to external (foreign) policy, security or criminal law. A separate Directive known as the 'Law Enforcement Directive' governs the data protection and data breach notification responsibilities of public authorities that process personal data in the context of criminal law. All EU member states have transposed this Directive, with the exception of Spain, which the Commission referred to the Court of Justice of the EU for not transposing EU law. In addition, in October 2018, the EU adopted Regulation 2018/1725, which covers and brings the EU institutions' data processing activities into line with the GDPR. This Regulation entered into force in December 2018, but it applied to Eurojust, the EU agency for judicial cooperation in criminal matters among national agencies, only as of December 2019.

Broad enforcement powers but practical resource constraints for DPAs.

The GDPR is meant to promote consistent and effective enforcement across the EU. It gives national DPAs strong investigative and enforcement powers, with the ability to impose high fines. DPAs are empowered to carry out data protection audits and they can require companies to provide access to their premises, their IT equipment and all personal data as necessary for the performance of their tasks. DPAs can order companies to bring processing operations into compliance with the GDPR and impose a temporary or permanent ban on specific processing operations. Non-compliance with a DPA's order may be subject to a fine of up to €20 million or 4 per cent of the company's total worldwide annual turnover, whichever is higher. The Belgian DPA was given these powers in December 2017, but it noted in its 2019–2025 Strategic Plan, released in December 2019, that it would require more budget and resources to exercise its powers effectively. Other DPAs are facing the same difficulties, which in July 2019 led the EC to urge national governments to allocate sufficient resources to them.

Problems with the one-stop shop and consistency mechanisms

Under the GDPR, the European Data Protection Board (EDPB), which includes all EU DPAs, the European Data Protection Supervisor who supervises the EU bodies' processing activities, and a representative of the EC, acts as an advisory body and is responsible for adopting binding decisions where DPAs disagree or fail to follow its advice. As an advisory body, the EDPB can adopt opinions regarding the 'one-stop shop' and the 'consistency' mechanisms in GDPR. To recall, the one-stop-shop mechanism is meant to identify a lead DPA to supervise a business established in several EU member states. The consistency mechanism creates a procedure to ensure consistent application of the GDPR among national DPAs. Between May 2018 and December 2019, more than 1,300 procedures were initiated to identify a lead DPA. The EDPB also issued more than 40 opinions under the consistency mechanism, including on DPAs' lists of processing operations for which no data protection impact assessment is required. These lists are helpful since they provide exceptions to the general GDPR requirement to carry out such assessments where a type of processing is likely to result in a high risk to the rights and freedoms of individuals.

Despite these statistics, the operation of both mechanisms has been criticised. The efficacy of the one-stop shop has been questioned, since there have been cases in which one company was fined by several DPAs, instead of being subjected to a single coordinated investigation. The EC is expected to discuss this issue in the context of its first biannual review of the GDPR. The covid-19 crisis has led to doubts about the DPAs' ability to work together consistently, given their disparate reactions. Although this reflects the uncoordinated reactions by EU member states to the pandemic more generally, the failure of DPAs to coordinate in this context calls into question whether GDPR has really been able to deliver a harmonised approach to the application and enforcement of its requirements.

Notification of security breaches and increased findings of adequate protection by non-EU jurisdictions

The GDPR requires all companies that process personal data to notify a security breach that is likely to result in a risk to the 'rights and freedoms' of the individuals concerned. Reports indicate that, from the entry into force of the GDPR in May 2018 to January 2020, around 160,000 personal data breaches were notified to DPAs within the European Economic Area (EU member states as well as Iceland, Liechtenstein and Norway), of which around 1,300 were notified in Belgium. To mitigate the risk of a security breach, companies are required to implement appropriate technical and organisational measures – such as pseudonymisation and encryption – to ensure a level of security that is appropriate to the risk.

"The NISD seeks to achieve a high common level of network and information system security across the EU; however, member states can impose more stringent requirements."

Importantly, this includes ensuring such security when transferring personal data outside of the EEA, including adopting appropriate measures where the transfer is made to a recipient country that has not been found to provide adequate protection by the EC. Although only a handful of countries are currently deemed to offer adequate protection (most of which had already been designated as such under the Directive that the GDPR replaced), their number is growing and is set to increase. The EC has recognised Japan as providing adequate protection in January 2019, and adequacy talks are ongoing with South Korea. India is reported to be seeking an adequacy finding by the EU, and EC officials consider that the 2019 Mercosur free-trade agreement makes the case stronger for adequacy findings to the benefit of Latin America countries. The EU is also considering entering into adequacy talks with neighbouring countries. However, the EDPB has shown very limited support for the EC to make an adequacy finding for the UK when Brexit takes full effect.

Belgian implementation

The Belgian Data Protection Act that was adopted in July 2018 to implement specific rules under the GDPR leaves GDPR security requirements unchanged. Non-compliance with these obligations may result in a fine of up to €10 million or 2 per cent of a company's total worldwide annual turnover, whichever is higher. In practice, though, DPAs will have to consider the gravity of and reaction to any data breach to ensure that the fines they impose are proportionate in light of the EDPB's 2017 guidelines.

From a cybersecurity point of view, the most interesting guidance from the Belgian DPA remains the one that it published in April 2018, on data protection impact assessments (DPIAs). The EDPB's 2017 guidelines on DPIAs set out the criteria to identify a 'high risk to the rights and freedoms of individuals'. While these criteria were still quite abstract, the Belgian DPA's guidelines go a step further and provide lists of processing activities that do or do not require a DPIA. For example, the Belgian DPA considers that a DPIA is always required for the large-scale processing of personal data of vulnerable individuals, such as children, for a different purpose than the one for which the data was collected. A DPIA is also required for large-scale processing of personal data where an individual's behaviour is observed, collected, established or influenced, including for advertising purposes, in a systematic manner and using automated means. The Belgian DPA considers that a DPIA is not required for the processing of personal data that is necessary to comply with a legal obligation, subject to a legal definition of the purposes of the processing, the categories of personal data processed and guarantees to prevent abuse, unlawful access or transfer. Another example of processing activity that does not require

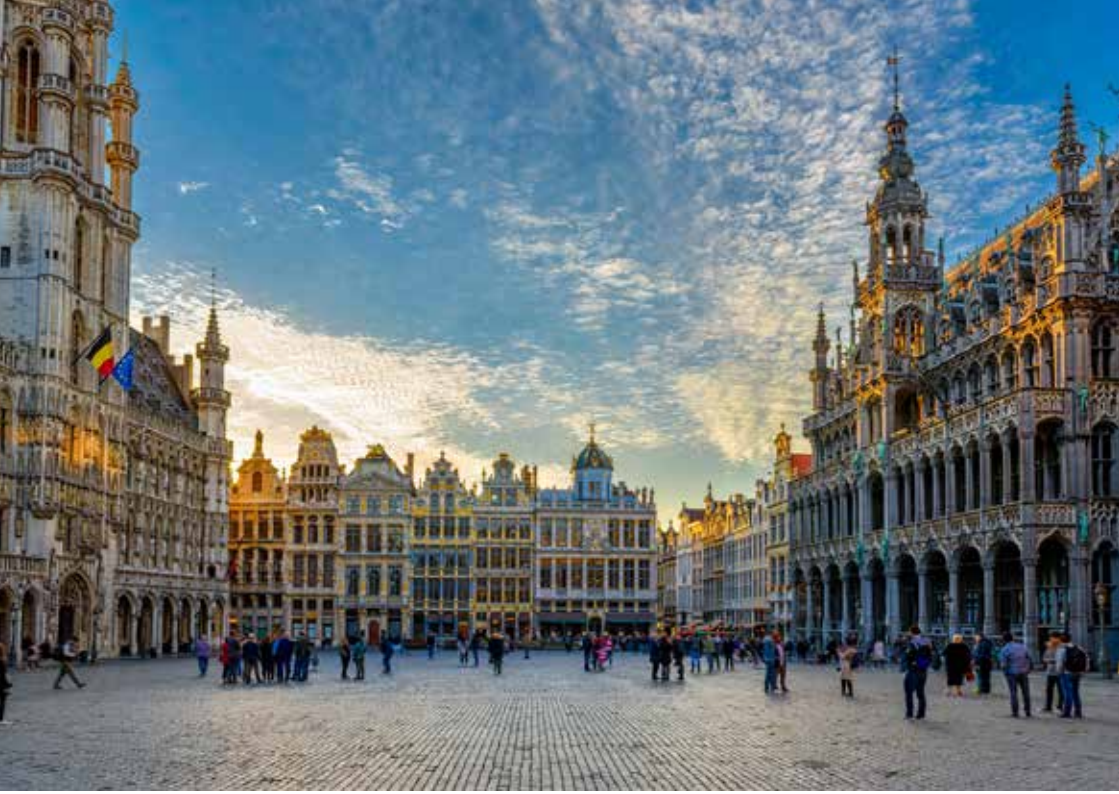
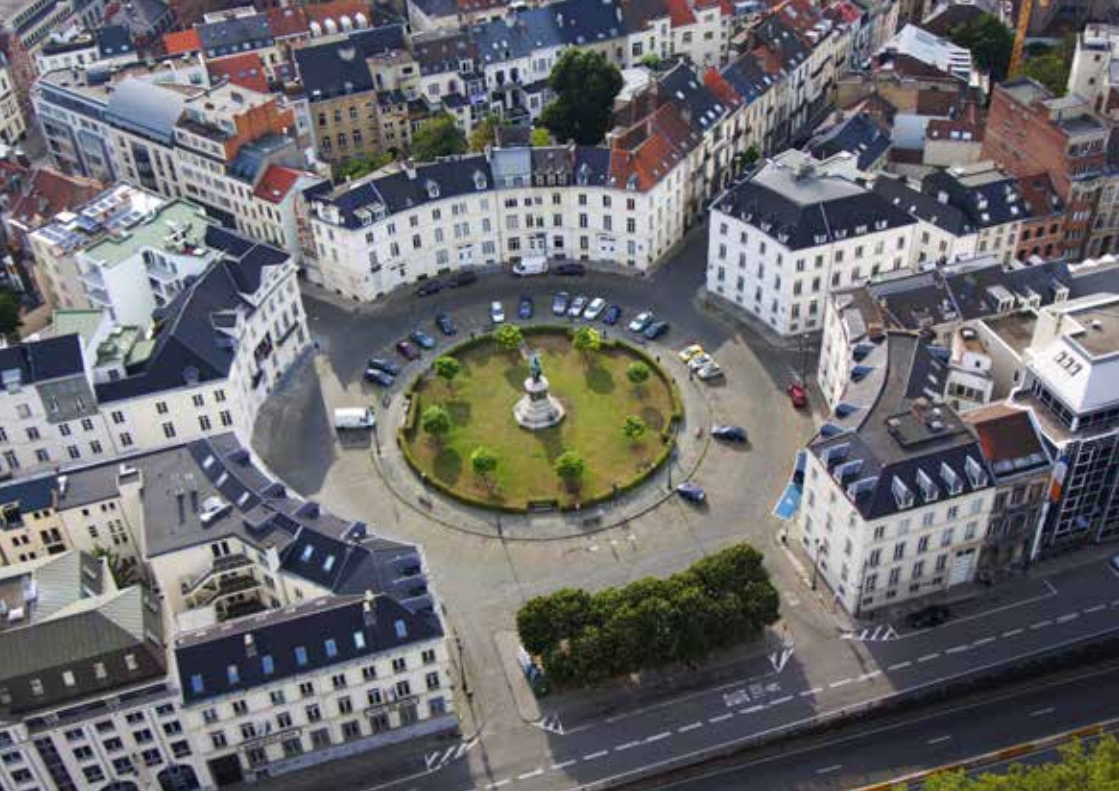


Photo: shutterstock.com/g/catarina

a DPIA according to the Belgian DPA is the processing of personal data that is necessary and exclusively restricted to the administration of employees' salaries, provided that such personal data is only shared with recipients who are authorised for this purpose and is not kept longer than necessary for the purposes of the processing.

Second, we examine developments affecting the NISD, which regulates cybersecurity standards for essential infrastructure at EU level. All member states have transposed the NISD into national law. The Belgian Network and Information Systems (NIS) Act entered into force on 3 May 2019. The NISD applies only to designated private and public-sector entities responsible for essential infrastructure in specific sectors. It does not extend to governmental information systems other than those used to operate essential infrastructure. The NISD seeks to achieve a high common level of network and information system security across the EU; however, member states can impose more stringent requirements. Each member state must adopt and communicate its cybersecurity strategy to the EC. The strategy should define the objectives, appropriate policy and regulatory measures to achieve this high level of security of the relevant NIS.



Identifying OES and possible expansion of DSP scope

Belgium is still in the process of revising the cybersecurity strategy that it had adopted in November 2012. In contrast to the GDPR, the NISD applies only to OES in specific sectors including energy, transport, banking, financial market infrastructure, healthcare providers, drinking water supply and distribution, and digital infrastructure (ie, internet exchange point, domain name system service providers and top-level domain name registries). The EU left it up to member states to identify OES that are established on their territory based on the criteria provided by the NISD. Belgium did so on 3 November 2019 but its list of OES is not publicly available for security reasons. In October 2019, the EC warned member states that the way they identified OES was sometimes inconsistent and that this could have a negative impact on the EU internal market.

The NISD also applies to digital service providers (DSPs), that is, online marketplaces such as eBay or Amazon, online search engines such as Google or Bing, and cloud computing services. For these operators, member states cannot go beyond NISD obligations in terms of security and notification requirements. The NISD does not apply to companies providing public communications networks or

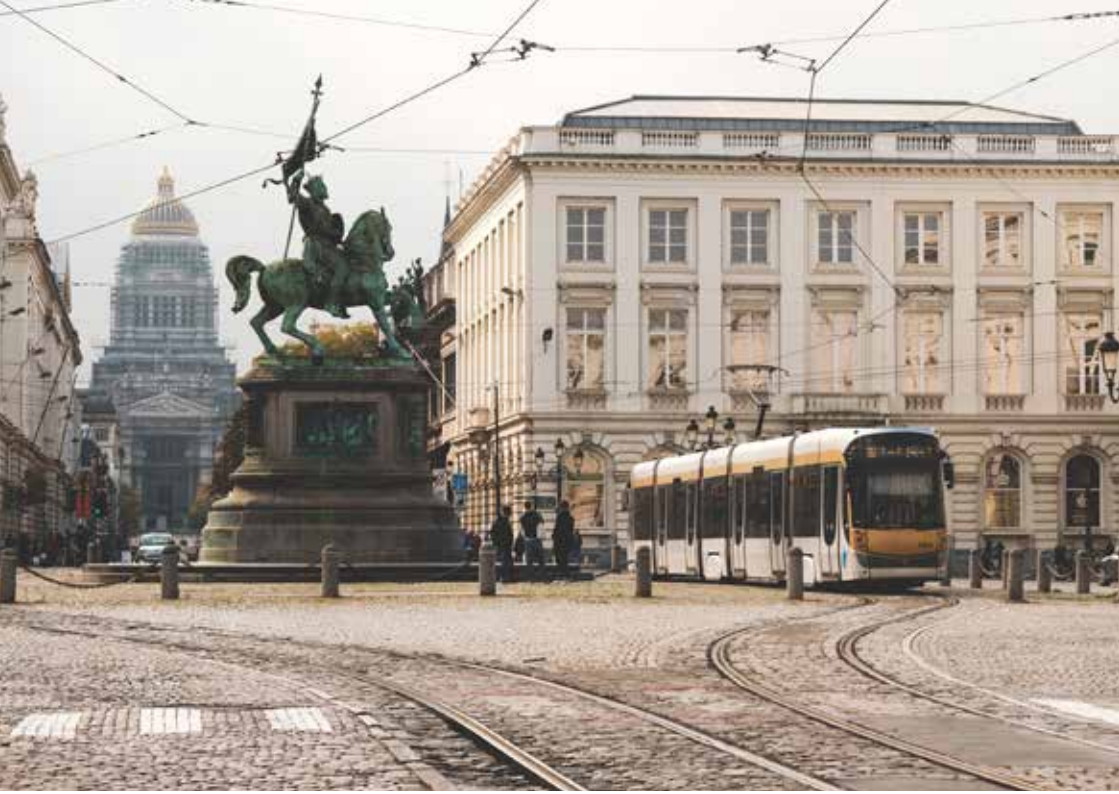
Photo: shutterstock.com/g/velvetes

publicly available electronic communications services, since these infrastructures are covered by the EECC. While the EC is seeking to finalise a review of the NISD by the end of 2020, ENISA's head already indicated that platforms and online marketplaces such as Facebook and Amazon might be included in a revised version of the NISD since they could be seen as 'critical infrastructures'. Other officials indicated that cloud-service providers may also fall within the scope of an updated NISD. The absence of any enforcement action since entry into force of the NISD is also raising questions and plays an important role in the context of the NISD review.

Companies falling within the scope of the NISD have two obligations that are similar to those under the GDPR. First, they must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. This includes preventing and minimising the impact of incidents affecting the security of their NIS to ensure their continuity. Second, companies covered by the NISD must notify incidents impacting their services without undue delay to the competent authority. A competent authority under the NISD can require OES and DSPs to provide the information needed to assess their security, including documented security policies and evidence of effective implementation, such as a security audit. Competent authorities can also issue binding instructions to OES to remedy their operations. Member states must adopt effective, proportionate and dissuasive penalties for infringements of the NISD. In Belgium, administrative fines could be as much as €200,000 and criminal sanctions can include up to three years of imprisonment and fines of up to €1.2 million.

Institutional structure

The NISD requires member states to designate one or more competent authorities to monitor the application of the Directive; a body responsible for coordinating NIS issues and acting as a single point of contact for cross-border cooperation at EU level; and a Computer Security Incident Response Team (CSIRT) that is meant to ensure the effective capacity to deal with incidents and ensure efficient cooperation at EU level. One entity can play all three roles – organisation of national cybersecurity agencies is left to national law. The NISD also promotes active cooperation among cybersecurity agencies at the EU level. An NIS Cooperation Group, composed of representatives from member states, the EC and ENISA, has been established and is meant to exchange best practices, discuss cybersecurity preparedness and evaluate national NIS security strategies, where requested. A network composed of national CSIRT representatives is meant to exchange information on CSIRT services and operations and issue guidelines for convergence of practices. ENISA is responsible for assisting the member states and the EC by providing its expertise and facilitating the exchange of best practices.



Belgium has a complex institutional cybersecurity scheme. The Belgian Centre for Cybersecurity (BCC) is the central authority for cybersecurity in Belgium and its Computer Emergency Response Team (CERT.be) received the CSIRT responsibilities, meaning that CERT.be has the operational responsibility for coordinating the response and providing support in the case of a cyber incident. Sector-specific authorities are in charge of the implementation of the law in their specific sectors, under the coordination of the BCC. For example, the Health Ministry acts as a sectorial authority for healthcare OES, while the National Bank of Belgium and the Belgian Financial Services and Markets Authority play the same role for financial OES. Each sectoral authority may have its specific CSIRT. The Belgian NIS Act sets up three levels of oversight of OES: controls at any time by sector-specific inspection services; annual internal audits; and external audits every three years by a certified body. Designated OES are required to adapt their information security policies by November 2020 and to implement them by November 2021.

Belgium has already launched several programmes to inform the public about cybersecurity risks and to promote solutions, such as the BCC's last anti-phishing campaign in October 2019, which reached almost half of the population. Belgium

Photo: shutterstock.com/g/aris_akritidis

had already adopted a National Emergency Cyber Plan prepared by the BCC and the government in late April 2017. The BCC's ongoing projects include delivering technical expert training to officials and taking fake websites offline on the basis of individuals' reports through suspicious@safeonweb.be. CERT.be offers its services on a 24/7 basis to companies and key sectors.

Third, we note the major reform of electronic communications regulation in the EECC, which was adopted on 11 December 2018. The EECC sets out, in a single unified Directive, the rules that apply to companies providing public communications networks or publicly available electronic communications services, including over-the-top services, irrespective of whether they process personal data. In particular, the EECC establishes three cybersecurity obligations for electronic communications services and network providers. First, such companies are required to take appropriate technical and organisational measures to manage the risks posed to the security of networks and services and to prevent and minimise the impact of security incidents on users and on networks and services. Second, they have to notify security incidents that have a significant impact on the operation of networks or services without undue delay to the competent authority. Third, electronic communications services and network providers must inform users potentially affected by a particular and significant threat pursuant to a security incident of any possible protective measures or remedies they can take. The EC, taking account of ENISA's opinion, may adopt decisions detailing the technical and organisational security measures to be adopted by providers, and the format and procedures applicable to the incident notification requirements. The EC has not adopted such decisions yet. Since the EECC is a Directive, all these rules must be transposed into national law by the member states. The deadline is 21 December 2020, but no member state has done this to date. ENISA is also supposed to facilitate the coordination of national rules to avoid diverging requirements.

Fourth, the EU adopted the Cybersecurity Act on 17 April 2019. The Act entered into force in May 2019, with a few provisions, including those dealing with national cybersecurity certification authorities, conformity assessment bodies and penalties, only entering into force in late June 2021. The Cybersecurity Act upgrades ENISA into a permanent EU agency for cybersecurity, while it used to operate on a fixed-term mandate that would require periodic renewal. The Act also creates an EU-wide certification framework for information and communications technology products and services. ENISA is getting more resources, in terms of both staff numbers and budget, and takes on additional responsibilities, such as organising annual pan-European cybersecurity exercises; advising member states on implementation of the NISD; and supporting and promoting EU policy on cybersecurity certification. ENISA is intended to be a centre of excellence and a resource for cybersecurity in the EU.

"Examples of covid-19 cyberattacks include fraudulent emails sent by criminals posing as the World Health Organization or coronavirus-themed phishing emails with infected attachments."

The new European cybersecurity certification schemes for ICT products, services and processes are intended to increase trust and security by attesting compliance with specified cybersecurity requirements. These certification schemes are also meant to address barriers in the single market caused by the existence of different national certification processes. The details of these certification schemes and requirements will be important to network and data service operators, including cloud computing service providers. ENISA has already been tasked by the EC to prepare a cybersecurity certification for cloud services and was expected to finalise it by the end of 2020 before the covid-19 crisis hit Europe. In January 2019, the EC also began preparatory studies to investigate the possibility of setting up a mandatory security certification for internet-connected devices.

Last, a word on the ePrivacy Regulation. This proposal was meant to replace the ePrivacy Directive at the time the GDPR entered into force but has gotten bogged down in the legislative process. It has lost significance in terms of cybersecurity since the European Parliament took out the security measures that it contained. This is because the draft ePrivacy Regulation security provisions added little to the framework provided by the GDPR, the NISD and the EECC. The latest version of the proposed e-Privacy Regulation, from late February 2020, maintains this position. There is growing scepticism about final adoption of the ePrivacy Regulation any time soon, if ever.

Moving to more specific cybersecurity concerns and debates, one cannot review what happened in 2020 without talking about the covid-19 crisis, since there is evidence that criminals have been exploiting the virus by launching online attacks. The risk proved to be even higher than anticipated with people moving to homeworking. Examples of covid-19 cyberattacks include fraudulent emails sent by criminals posing as the World Health Organization or coronavirus-themed phishing emails with infected attachments containing fictitious safety measures or links to malicious websites. In reaction, DPAs and cybersecurity centres in Europe have been urging businesses and people working from home to follow online safety advice and to take precautionary measures, such as using VPNs, avoiding the storage of files locally and connecting remotely to their company's own servers.

The contact-tracing apps that members states developed to fight the spread of the virus and support deconfinement measures also raised cybersecurity issues. After a series of confused and disorderly national reactions, the EC, with the EDPB's help, issued guidance regarding the use of such apps. The guidance included cybersecurity recommendations, such as ensuring that the apps store data on the individual's terminal device using state-of-the-art cryptographic techniques or that access should be logged if the data were to be stored in a central server. All transmissions from the personal device to the national health authorities should also be

encrypted. The EC insisted that apps should work using Bluetooth to the exclusion of any other location services to avoid tracking by third parties. The EC also expressed its preference for using temporary user IDs that change regularly rather than the actual device ID during the collection of proximity data. Finally, the EC recommended that the source code of the app should be made public and available for review and it encouraged the automatic deletion or anonymisation of the data after a certain point in time. The Belgian Data Protection Authority said that the legislation that sets up the Belgian contact-tracking system should be 'fundamentally reviewed' because it lacks clarity, consistency and necessity. It therefore remains to be seen where this will lead us in Belgium.

In addition, 5G has been at the heart of recent cybersecurity discussions. This is because 5G is expected to raise bigger security risks than 3G or 4G since it offers more potential entry points for hackers owing to a less centralised architecture, smart computing power at the edge, the need for more antennae and increased dependency on software. In this context of technical transition and China's rise to prominence, the EU has expressed concern about the involvement of Chinese companies, especially Huawei, in the build-out of EU member states' 5G network. In March 2019, the EC issued a recommendation on the cybersecurity of 5G networks, followed by a toolbox to mitigate the risks raised by 5G networks in January 2020. The toolbox includes strategic measures (eg, assessing the risk profiles of suppliers or ensuring the diversification of vendors), technical measures (eg, ensuring strict access control and secure network management) and supporting actions (eg, reinforcing testing and auditing capabilities). EU regulators are also helping. In its 2021–2025 strategy released in March 2020, the Body of European Regulators for Electronic Communications (BEREC) noted that it helped with the development of the EC toolbox and that it will continue to share information and experience on electronic communications to help address the cybersecurity risks raised by 5G. ENISA is expecting the EC to ask it to develop an EU-wide 5G cybersecurity certification.

Artificial intelligence (AI) is also a developing topic with cybersecurity implications. ENISA is concerned that AI and its application in automated decision-making might open up new avenues for manipulation and attack, creating new cybersecurity challenges. Consequently, in March 2020, ENISA launched a call to bring together a multi-disciplinary group of experts to advise it on AI cybersecurity topics. The EC shared its vision of AI and provided a roadmap of the rules that businesses may have to comply with in the near future in a White Paper released in February 2020. The paper was open for public consultation until May 2020 and the EC planned to publish an assessment list to help companies verify the application of key AI requirements by June 2020, but the covid-19 crisis could delay this timetable. Although it is unclear when EC policy proposals would be turned into formal legislative texts, the process to

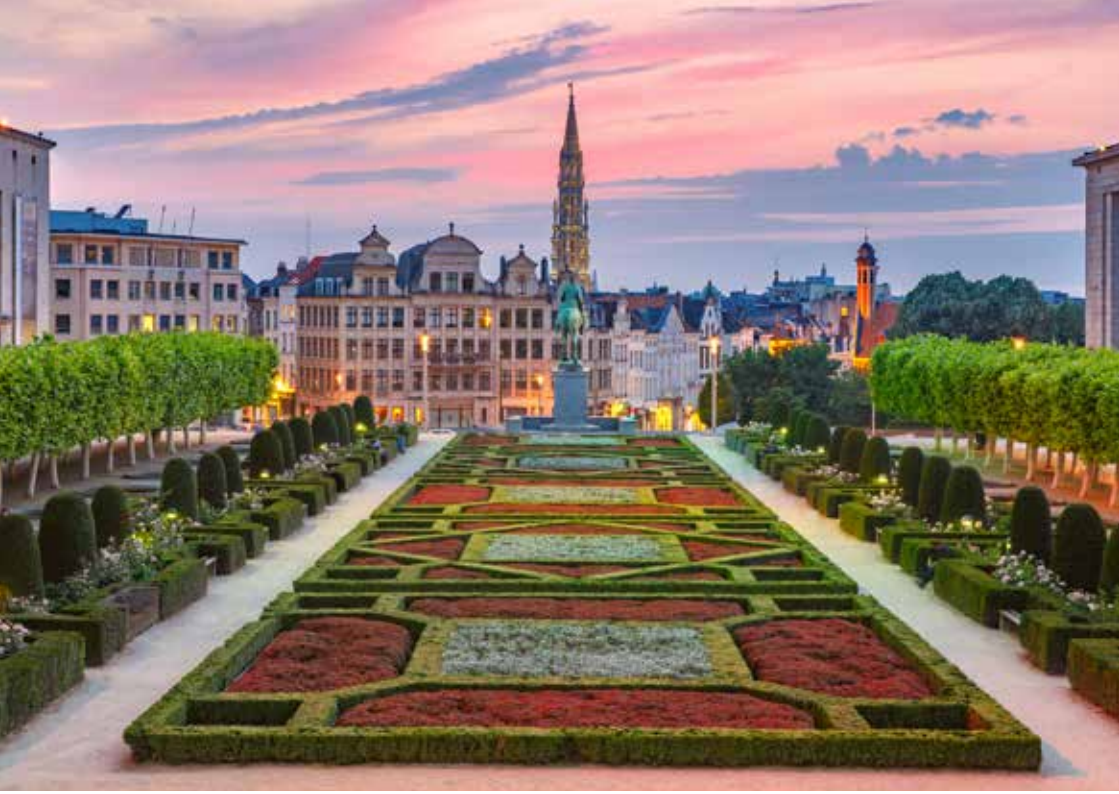
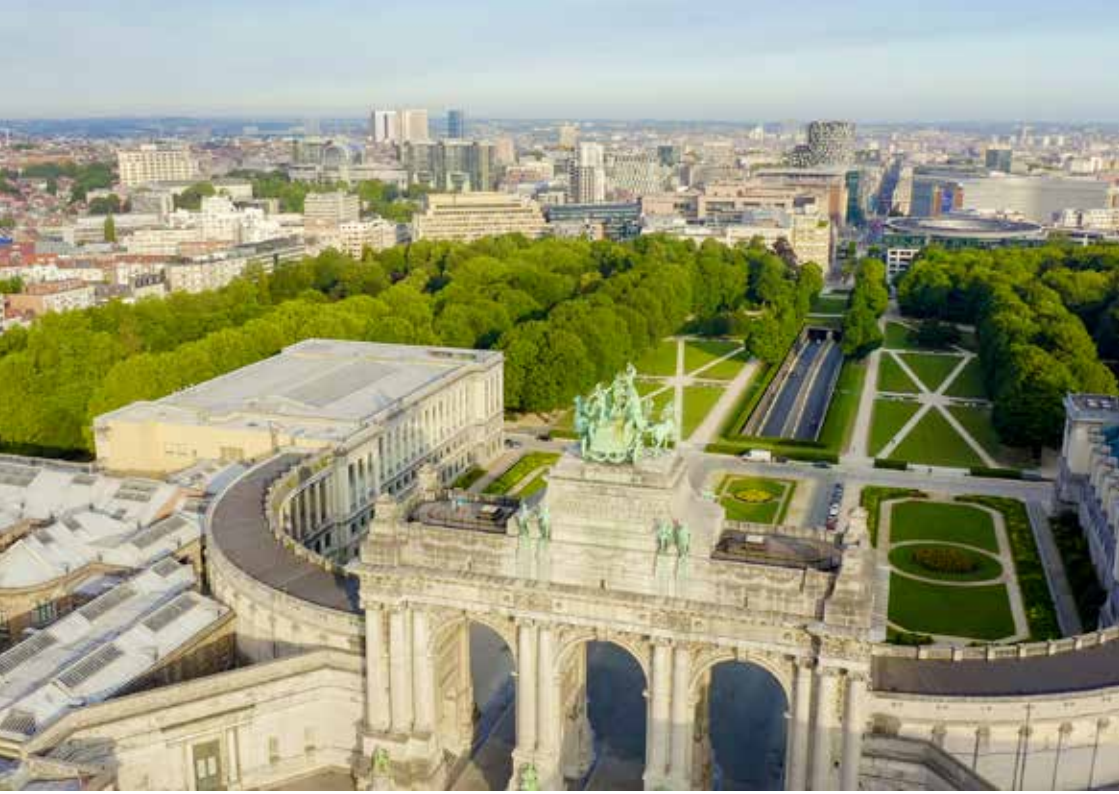


Photo: shutterstock.com/g/olgacov

regulate AI in the EU has begun and will include cybersecurity aspects. In particular, the EC would like to clarify liability rules for all players in the AI supply chain and for all AI-specific types of risk, such as cyberthreats or risks that result from the loss of connectivity. The EC believes that clarifying liability in advance is important, since risks may be present at the time products are placed on the market. They may also arise as a result of software updates or self-learning when the product is being used.

With regard to connected vehicles, the EC is concerned that connectivity and system integration of components originating from different sources may bring new threats of cyberattacks, such as hackers taking remote control of a vehicle. Although the GDPR applies to the processing of personal data collected from vehicles, there is no EU sector-specific approach yet on the protection of vehicles against cyberattacks. The EC, therefore, launched a public consultation on connected and automated vehicles in November 2018, asking for input on the need to put into place regulatory measures to secure connected and automated vehicles against cyberattacks; the need to require automobile manufacturers to take responsibility for taking protective measures themselves; and the kinds of action that should be prioritised to increase cybersecurity resilience. ENISA published good practices for the security of smart



cars in November 2019 to identify the relevant assets, the emerging threats targeting such cars and the potential security measures and good practices to mitigate them. The EDPB also published draft guidelines on connected vehicles in February 2020, recommending that the industry adopt security measures such as using encryption key management systems that are unique to each vehicle and regularly renewing encryption keys. The EDPB also made specific recommendations to vehicle manufacturers, such as partitioning the vehicle's vital functions from those relying on telecommunication capacities (eg, 'infotainment') and storing a log history of any access to the vehicle's information system so as to be able to understand the origin of any potential attack and periodically carry out a review of the logged information to detect possible anomalies. It is expected that these initiatives will lead the EU to adopt specific legislation for connected vehicles in the future.

In terms of online payments, the new EU Payment Services Directive (PSD2) went into full effect on 14 September 2019, but due to delays in implementation, the European Banking Authority allowed for an extension until 31 December 2020. PSD2 imposes security requirements for electronic payments and the protection of consumers' financial data. In particular, PSD2 requires banks to implement

Photo: shutterstock.com/g/maykova+galina

multi-factor authentication for all proximity and remote transactions, which should use two of the following three features: something only the user knows (eg, a password); something only the user possesses (eg, a smartphone); or something only the user 'is' (eg, a fingerprint).

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

Under the GDPR, companies must generally notify any data breach to the DPA within 72 hours where it is likely to result in a risk to the rights and freedoms of individuals. These risks include discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, reputational damage or any other significant economic or social disadvantage; disclosure of sensitive personal data (identifying the race, ideology, health, sex life or criminal record of an individual); profiling data (work performance, creditworthiness, personal interests); personal data of vulnerable individuals (eg, children); or a disclosure that simply prevents the future exercise of control over personal data. Risks are viewed as higher under the GDPR where processing concerns big data.

Companies must also disclose a breach directly to the individual concerned without undue delay where that breach is likely to result in a 'high risk' to the individual's rights and freedoms. Companies do not have to disclose a breach to the individual concerned where the data affected by the breach was protected (eg, through encryption); or if they have taken subsequent measures that ensure that a high risk is no longer likely to materialise; or if such disclosure would involve a disproportionate effort. In the latter case the company must, however, issue a public statement disclosing the breach. Companies that process personal data on behalf of another company must notify the breach to their customers. DPAs also have the authority to order companies to communicate a personal data breach to the individual concerned in appropriate circumstances, such as where the DPA views the breach as resulting in a 'high' risk and not just a risk.

The EDPB has already published guidelines to help companies understand the breach notification requirements. These guidelines recommend that companies consider specific criteria when assessing whether there is a risk or a high risk. These criteria include the type of breach, the nature, sensitivity and volume of personal data, how easy it is to identify individuals, the severity of consequences of the breach for individuals, special characteristics of the individual concerned and the company in question and the number of affected individuals. The guidelines also specify when a data controller or processor should be deemed to be aware of a breach, since

that triggers the countdown to the deadline for notifying the breach, if required. Guidance on the identification of these risks can also be provided by approved Codes of Conduct (CoCs) or certifications, or by EDPB guidelines. CoCs are likely to be of particular interest, since they could offer a degree of compliance comfort on a cost-efficient basis. The EDPB adopted guidelines on CoCs and certifications in June 2019, but it will probably take some time before companies start obtaining approvals for CoCs or certifications. Still, it is generally recommended for companies to err on the side of caution, notifying breaches to the DPA and discussing with the DPA whether they should also notify the breach to the individuals concerned.

Under the EECC, member states must ensure that companies providing public communications networks or publicly available electronic communications services notify the national competent authority without undue delay of a breach of security that has had a significant impact on the operation of their networks or services. To determine the significance of the impact of a security incident, providers of public communications networks and publicly available electronic communications services should take into account the number of users affected, the duration of the incident, the geographical spread of the area affected, the extent to which the functioning of the network or service is affected and the extent of impact on economic and societal activities. The competent authority in one member state may inform the competent authorities in other member states. It can also inform the public, or require the providers to do so, where it determines that disclosure of the incident is in the public interest. It is for each member state to decide which national authority will be responsible (eg, the communications regulator or the DPA).

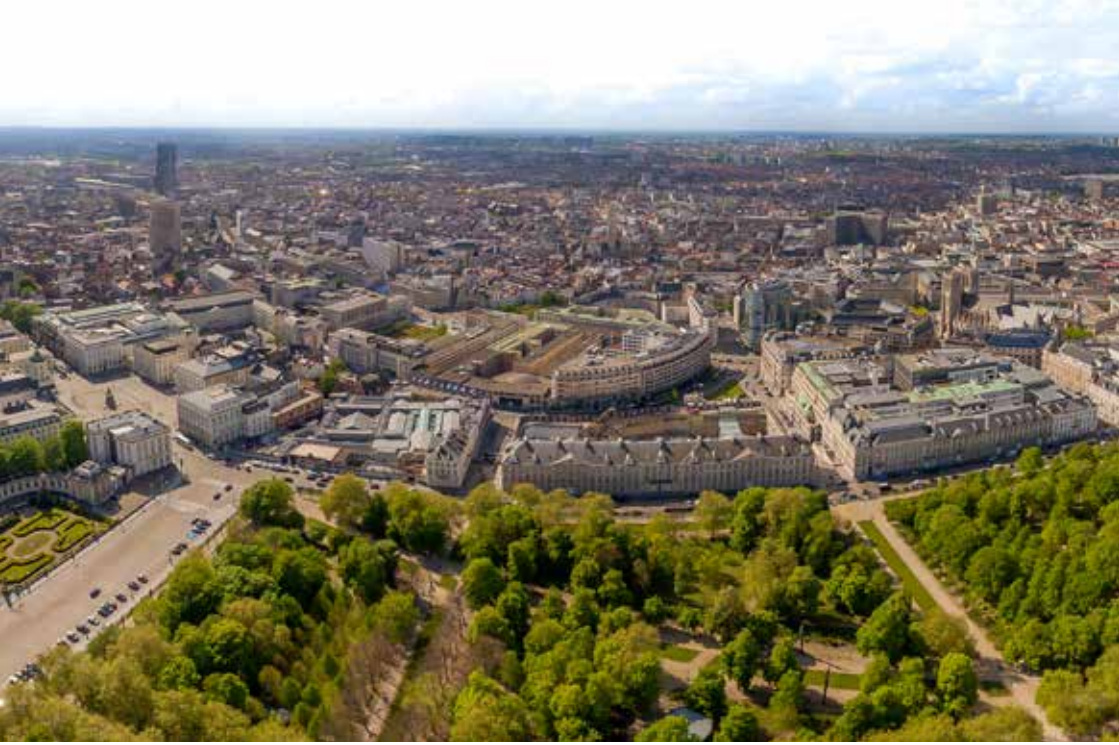
Belgium has yet to transpose the EECC into national law, so the current breach notification scheme for electronic communications services and networks providers might change. Currently, Belgian law sets up a twofold notification obligation: providers of publicly available electronic communications services must inform their subscribers and the Belgian Institute for Postal services and Telecommunications (BIPT) of a particular risk of breach of network security. In 2014, the BIPT issued a decision that specifies when and how operators must notify it of a security incident. Service providers must also inform the Belgian DPA of a breach of personal data, which in turn notifies the BIPT. They must inform their subscribers of a breach of personal data where the criteria in the EU rules described above are met.

Under the NISD, companies must notify incidents impacting their services to the competent authority. OES must notify incidents having a 'significant' impact on the continuity of their services to the authority, while DSPs must notify incidents having a 'substantial' impact on their services. Criteria to determine whether an incident is significant or substantial include the number of users affected, the duration of the incident and its geographical spread and, for substantial incidents, the extent of the

"Best practices to improve cybersecurity preparedness include internal procedures for reporting breaches, an internal response plan, an incident response team and training of personnel."

disruption to the functioning of the service and the extent of the impact on economic and societal activities. Since these criteria are quite broad, it is expected that they will be refined through practice. There are also provisions for voluntary notification of incidents by entities that are not listed as OES or DSPs. After consulting with the company, the notified competent authority may inform the public about an incident where public awareness is necessary to prevent or deal with it or, with regard to DSPs, where disclosure of the incident is in the public interest.

In Belgium, the 12 April 2019 Royal Decree provides further clarification on breach notifications for OES and DSPs. Incidents must be notified to CERT.be, the sector authority or its sectorial CSIRT (eg, the Ministry for transport for an airline company), and the Belgium Crisis Centre, which is responsible for addressing crisis and emergency situations at national level in Belgium. The Royal Decree has created a breach notification platform to that end. Separate voluntary notification of a data breach to CERT.be is also possible. This can provide the basis for benefiting from CERT.be's expertise to limit the damage caused by the breach and avoid future incidents. It also allows CERT.be to identify trends for cyber incidents and further develop specific solutions at the national level.



3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

As in other areas, an ounce of prevention is worth a pound of cure. Companies should make sure that they continuously invest in their own data security and stay abreast of cybersecurity developments as well as their evolving legal obligations.

If an incident occurs, whether an attempted data breach or a successful breach, the first concern should be to identify the scope of the incident and to make sure that the network is secured. An incident response team should be set up to assess the situation, prevent expansion of an identified data breach, secure relevant information systems and then try to recover the data concerned. Private sector advisers as well as public authorities can support companies in this process.

In a second step, the company will need to determine whether it is under an obligation to notify a data security incident to the competent authority or affected individuals. Even if not under an obligation to do so, such notifications may be advisable in many cases. As described above, companies face broad notification obligations under the GDPR and the NISD – in particular, where a data breach creates

Photo: shutterstock.com/g/photolondonuk

risks for individuals, or has a significant impact on continuity of services for an OES or a substantial impact on services for a DSP.

Third, despite the guidelines of the EDPB and the Belgian DPA, it may not be easy to identify when a company should be deemed to be aware of a breach. This means that companies may face difficulties identifying the deadline for notifying the breach.

A fourth and closely related issue consists of appropriately preparing to be able to make relevant notifications within the short time periods that will apply. The GDPR provides that companies must notify the security breach to the authority within 72 hours. If this time frame is not feasible, companies should notify the breach without undue delay and provide a reasoned justification for the delay. The NISD provides for OES and DSP notification without undue delay, rather than specifying a minimum time period.

It is not enough to notify the breach; certain information must be gathered and provided to the regulators. The GDPR provides that notification to the authority must at least describe the nature of the personal data breach, including the number and categories of data subjects and personal data records affected; provide the Data Protection Officer's contact information; describe the likely consequences of the personal data breach; and describe how the controller proposes to address the breach, including any mitigation efforts. If all of this information is not available immediately, it may be provided successively as long as there is no undue delay. Collecting and providing the relevant information within 72 hours may be challenging, hence the need for teams that are prepared and can follow appropriate policies on who should be contacted within the company, how the authority should be notified and how communication with customers should occur.

Under the NISD, less information is required for notification, but it should include sufficient detail to enable the competent authority or the CSIRT to determine whether there is any cross-border impact and the degree of significance of cross-border impact for DSPs.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

Best practices to improve cybersecurity preparedness include internal procedures for reporting breaches, an internal response plan, an incident response team and training of personnel. Large companies view a written information security policy as best practice. This is also useful in documenting existing data security measures when notifying data processing operations to the DPA. A few companies have also implemented additional measures, such as regularly testing their breach notification plans.

Best practices also include more general compliance with international cybersecurity standards, such as ISO 27001 or CoCs. Cloud service providers, for example, have long been sensitised to cybersecurity requirements by the nature of their business. Thus, in 2017, SCOPE Europe, an association supporting the co-regulation of the information economy, started developing a CoC for the cloud computing industry (the EU Cloud CoC) with the EDPB's help. This Code includes cloud service providers' commitments to ensure security and notify breaches to competent authorities. The Code also includes a governance structure intended to support its effective implementation. Members of the EU Cloud CoC include Alibaba Cloud, Cisco, Fabasoft, Google Cloud, IBM, Oracle, Salesforce, SAP and TrustArc. In April 2019, SCOPE Europe released the latest version of the EU Cloud CoC after several revisions meant to align its provisions with the GDPR and to take into account the EDPB's guidelines on CoCs, as well as the DPAs' input. SCOPE Europe then announced that it would submit the CoC for approval to DPAs. In August 2019 and February 2020, SCOPE Europe announced that Workday and Epignosis were the first cloud service provider and eLearning service provider to demonstrate adherence to the EU Cloud CoC, respectively.

Another organisation, the Cloud Infrastructure Services Providers in Europe (CISPE), represents 30 cloud infrastructure providers operating in Europe, mainly European small and medium-sized enterprises (SMEs) headquartered in over 15 member states, representing collectively more than 100 cloud infrastructure services. CISPE created its own CoC in September 2016. The latest version published on CISPE's website is dated January 2017. This Code goes beyond GDPR requirements, as it guarantees that participating organisations will provide customers with the ability to choose to use their services to store and process data entirely within the EEA. The EDPB gave substantial feedback to CISPE in February 2018 and made suggestions to improve the Code, which it viewed as making a positive first impression. The objective of CISPE is also to have the Code approved by EU DPAs and make it the benchmark standard for the industry. CISPE is, therefore, revising its Code in light of the comments received.

In Belgium, the BCC has also published a Cyber-guide reference in February 2018, in cooperation with the Belgian Cyber Security Coalition, a cross-sector collaboration between public authorities, companies, professional organisations and universities. The coalition released an updated kit for internal cybersecurity awareness in May 2018, and a Cyber Security Guide for SMEs as well as a Cyber Security Incident Management Guide in 2016. Best practices have been developed by a joint private sector or academic initiative that is led by the Federation of Belgian Enterprises, the International Chamber of Commerce in Belgium, Microsoft, Ernst & Young and the cybercrime centre of the University of Leuven. This group published

"Companies thinking about moving personal data to a cloud hosting environment should consider two threshold issues: where is the cloud server located and how is the data going to be protected?"

the Belgian Cyber Security Guide in 2014. The guide is intended to convince businesses of the importance of being prepared for cyberthreats and offers advice that is adapted to a company's size or role (eg, large national companies trading internationally, medium-size retailers with an online presence, SMEs in the accounting sector or Belgian start-ups). The guide lists 10 'security key principles' and 10 'must-do security actions', including user education and awareness, protection of information, updating systems, use of mobile device security, enforcement of safe surfing rules and access to information on a 'need to know' basis. A checklist can be used by companies to assess whether they are sufficiently equipped for cyber incidents.

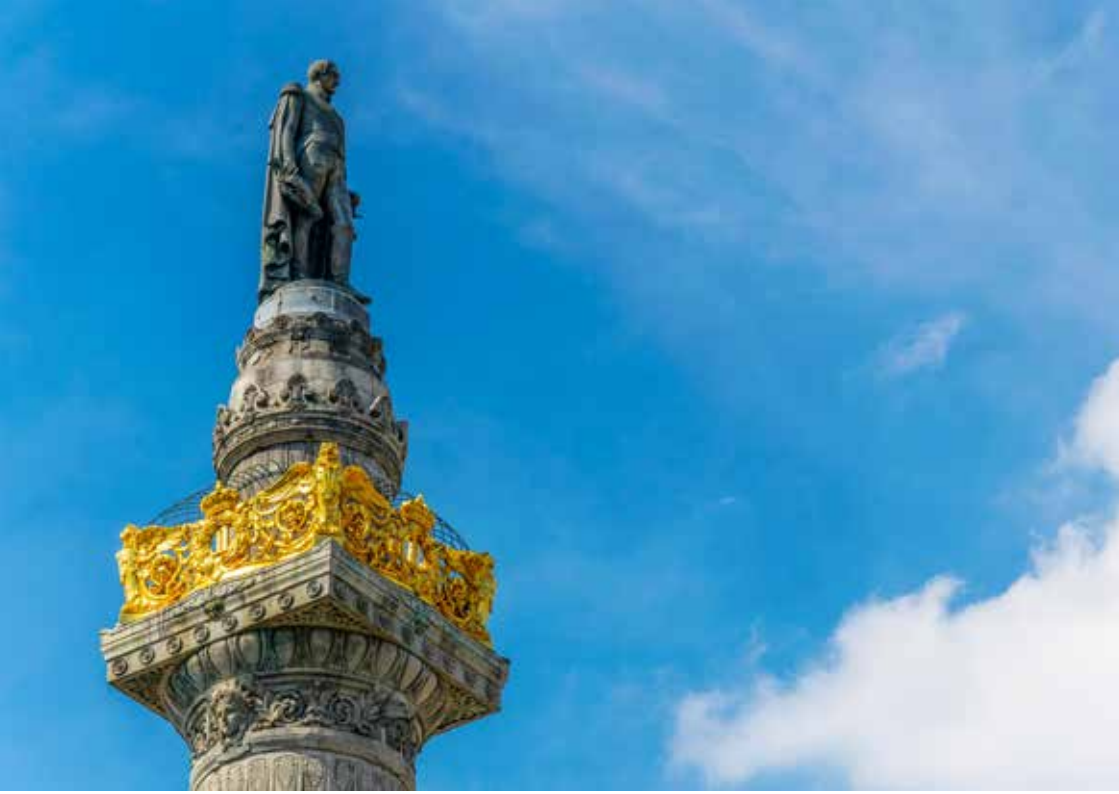
In the financial services sector, the Belgian National Bank (BNB) has focused on increasing cyber resilience by improving risk management and intensifying the use of internal tests within companies to assess the level of cybersecurity preparedness. In December 2015, the BNB adopted a circular on management of cyber risks that is binding on the Financial Market Infrastructures (FMIs) that are established in Belgium. The circular entered into force in January 2016. The Bank for International Settlements and the International Organization of Securities Commissions published similar recommendations on this topic in June 2016. The BNB also contributed to

the publication of the European Bank Authority's recommendations on outsourcing to cloud service providers. More recently, in November 2018, the BNB adopted the TIBER-BE Framework in the context of a larger European initiative to mimic potential attacks by real high-level threat groups and test whether the defensive measures taken are effective, thus supplementing the periodic information security audits.

The BNB carries out controls to determine whether FMIs established in Belgium comply with the circular. In particular, the circular requires companies to adopt a security plan that covers data integrity, notes reporting rules and expectations, contains criteria to identify critical activities and resources, specifies training measures and sets out internal control measures where subcontractors are employed. FMIs must create a governance system to keep the complexity of their IT systems at a manageable level and avoid harm to data security. FMIs must also evaluate personnel with access to data for their integrity, reliability and knowledge about data security. The BNB expects to be informed rapidly and adequately of any incident that has a serious impact on data security or operational continuity for critical activities of FMIs. Additionally, an internal report on an FMI's critical activities, services and resources must be kept up to date. In practice, the BNB has already led a number of inspections to verify compliance with the regulatory framework and the appropriate management of IT systems regarding cyber risks. Finally, the BNB is involved in the sector-specific initiatives in the field of cyber risks. For example, it contributes to the creation of a framework for red teaming (ethical hacking) in the context of the Belgian Financial Sector Cyber Advisory Council and the European Central Bank's Cyber Security Strategy.

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

Moving data to a cloud hosting environment may create additional risks for data security and privacy because of the data transfers required and reliance on external systems. On the other hand, specialised cloud hosting service providers will have invested heavily in data security since this is core to their business and the services they provide. By contrast, data security is simply a cost and compliance obligation for companies active in other sectors of the economy. A cloud-hosting provider may well offer a more robust platform in terms of data security than its customer could or would want to. Nevertheless, the GDPR imposes additional requirements on the use of external processors by data controllers. Companies thinking about moving personal data to a cloud hosting environment should consider two threshold issues: where is the cloud server located and how is the data going to be protected?



With regard to data security in the cloud, companies must ensure that their cloud service provider provides sufficient guarantees that it has implemented appropriate technical and organisational measures to ensure that processing will meet GDPR requirements. To that end, companies must conclude a binding contract with their cloud service provider, specifying, among other things, that it will assure the level of data security required under the GDPR. Again, adherence to an approved CoC or an approved certification can be used by cloud service providers to demonstrate compliance.

The Belgian DPA issued an opinion regarding the use of cloud service providers in October 2016. The DPA recommends identifying potential risks prior to moving data into a cloud. Access of the cloud service provider to the data should be limited to a strict minimum. The employees of the cloud service provider should sign a confidentiality clause with their employer. The cloud service provider should also contractually commit not to share the data with third parties, except if it uses subcontractors (which must observe all the same obligations vis-à-vis the cloud service provider as it has as regards the data controller). Moreover, the contract between the data controller and the cloud service provider should state that any data breach must be immediately reported to the data controller. More generally, the DPA advises

Photo: shutterstock.com/g/pavel+dudek

"Non-compliance with transfer restrictions will be subject to fines under the GDPR of up to €20 million or 4 per cent of a company's worldwide annual turnover, whichever is higher."

that companies should track every party's precise involvement in the processing operation to determine liability in the case of a data breach. Both the data controller and the cloud service provider can be held responsible under the Belgian Data Protection Act where they do not take appropriate measures to ensure data security.

The location of data is very important, as confirmed in the Belgian DPA's opinion. Under the GDPR, companies are prohibited from transferring personal data outside the EEA unless the recipient country has been found to provide adequate protection by the EC, or the company has adopted appropriate alternative instruments to commit to adequate protection. Such instruments can consist of SCCs published by the EC; binding corporate rules (BCRs) for intra-company transfers (ie, an internal CoC defining a company's policy regarding data transfers from businesses to their affiliates located out of the EEA that has been approved by a DPA); or an approved certification or adherence to an approved CoC where the controller or processor located outside the EEA submits to jurisdiction and legal process in its home country to ensure enforceability of a data subject's rights.

Until July 16, 2020, transfers to the US could rely on participation by the US entity in the Privacy Shield (more than 5,300 US companies rely on this instrument to

date). However, on 16 July 2020, the ECJ ruled that the Privacy Shield is incompatible with EU law. This judgment contrasts with the EC's report on its third annual review of the Privacy Shield released in October 2019. Because of major improvements, the EC had concluded that the Privacy Shield continued to ensure an adequate level of protection for personal data transferred from the EU to the US. The EC had noted that the US Department of Commerce was ensuring the necessary oversight in a more systematic manner by regularly verifying that companies comply with the Privacy Shield principles and that the US Federal Trade Commission had also taken several enforcement actions. In addition, the US government had appointed an independent ombudsperson and additional members or the Privacy Civil Liberties Oversight Board, ensuring that the Board, which ensures that the US government's counterterrorism laws are balanced with privacy concerns, is fully staffed for the first time since the adoption of the Privacy Shield.

SCCs have also been challenged in court proceedings. The Irish High Court agreed that there were well-founded concerns about the protection of personal data transferred to the US pursuant to SCCs and referred the case to the ECJ for a preliminary ruling on their validity. In December 2019, the advocate general in charge of advising the ECJ on this case concluded that SCCs are valid.

On 16 July 2020, the ECJ confirmed that SCCs are still valid, but it made them practically impossible to use for transfers of personal data from the EU to the US. This is because the ECJ considered that SCCs cannot be used where the legislation of the recipient country does not allow the data importer to comply with the SCCs, in particular because such legislation allows its public authorities to interfere with individuals' data protection rights. This would appear to apply to the US, given domestic intelligence agencies' broad surveillance powers. The judgment therefore creates great legal uncertainty for companies engaged in EU-US data transfers, with as yet unclear alternative solutions. The existing SCCs were drafted under the previous EU data protection Directive and have not been updated since the GDPR replaced it. In its 2020 contribution to the annual review of the GDPR, the EDPB therefore indicated that there is a pressing need for the EC to bring the existing set of SCCs in line with the GDPR and to draft additional SCCs to cover new transfer scenarios. The ECJ's judgment will increase the pressure on the EC to do so.

Companies should, therefore, identify the location of the cloud service provider's servers to determine whether additional instruments should be put into place to ensure adequate data protection. Again, the ECJ's judgment on SCCs and the US Privacy Shield is not helpful in this regard. Non-compliance with transfer restrictions will be subject to fines under the GDPR of up to €20 million or 4 per cent of a company's worldwide annual turnover, whichever is higher.

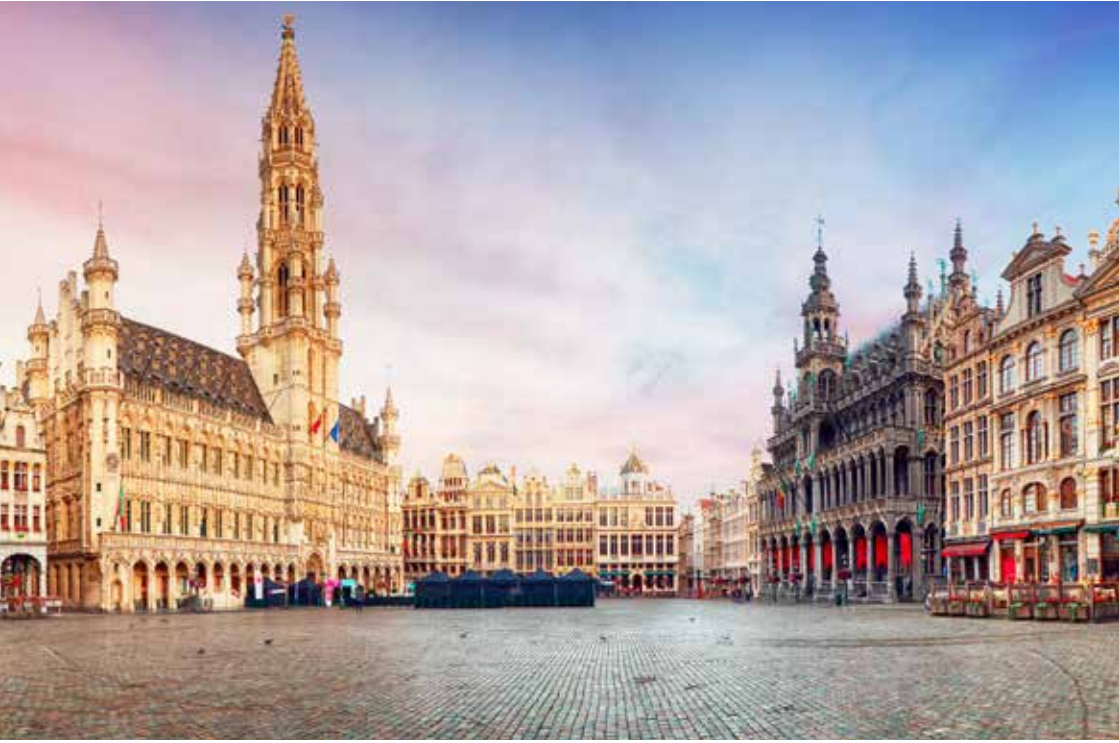
6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

The EU Cybercrime Directive, which came into force in August 2013 and has been transposed into national law by all member states, establishes four main offences: (1) illegal access to information systems; (2) illegal system interference; (3) illegal data interference; and (4) illegal interception. The Directive also makes it a criminal offence to produce, sell, procure for use, import, distribute or otherwise make available software designed or adapted primarily to committing these offences. This includes making available a computer password, access code or similar data through which an information system can be accessed with the intention of committing any of these offences. Member states must take the measures required to ensure that these offences are punishable by effective, proportionate and dissuasive criminal penalties.

The Cybercrime Directive also provides rules about increased cooperation between competent authorities. Member states must ensure that they have an operational national point of contact and that they make use of the existing network of available operational points of contact. Member states must also ensure that they have procedures in place so that urgent requests for assistance receive a response within eight hours, at least as to whether the request will be answered, in what form and with what timing. The Directive also lays down basic rules for the definition of criminal offences and provides that member states must have effective, proportionate and deterrent sanctions for such offences.

At the EU level, Europol, the EU agency for law enforcement cooperation, set up the European Cybercrime Centre (EC3) in 2013 to strengthen law enforcement response to cybercrime in the EU. The EC3's approach is based on three prongs: forensics, strategy and operations.

Belgium was one of the first member states to establish criminal offences (ie, hacking, cyber sabotage, cyber fraud and cyber forgery) for cybercrimes in its Criminal Code in 2000, but one of the last to implement the Cybercrime Directive in July 2017, after an increase in human resources within the Regional Computer Crime Units and the Federal Computer Crime Unit of the police. Sanctions for internal and external hacking are up to five years in jail or penalties of up to €400,000, or both. Sanctions for providing the means to hack a system are up to three years in jail or penalties of up to €800,000. Sanctions for instructing someone to hack a system are up to five years in jail or penalties of up to €1.6 million. There also are sanctions for knowingly possessing, disclosing, sharing or otherwise using hacked data (up to three years in jail or penalties of up to €800,000). Sanctions for cyber sabotage are up to five years in jail or penalties of up to €800,000. Sanctions for cyber forgery and cyber fraud are up to five years in jail or €800,000. All of these sanctions can



be doubled where they are committed less than five years after a conviction for the same offences. The Belgian Code of Criminal Procedure also provides authorities with several instruments to investigate cybercrime offences, including the interception and tracing of electronic communications, the identification of users of electronic communications services, the seizure of data and network searches.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

M&A deals can heighten the risk of a cyberattack by creating an attractive target – the proposed deal. Since such deals involve the sharing of very large volumes of commercially sensitive information (eg, bid prices, confidential business information gathered and stored in data rooms, negotiation strategies, the acquisition decision itself, potential synergies and future expansion plans), companies involved in the deal should make sure that due diligence repositories and the deal process are well protected.

More substantively, it is very important that companies include cybersecurity and data protection checks in their due diligence programme. This means that the acquirer should check whether the target complies with Belgian or EU data

Photo: shutterstock.com/g/ttstudio

protection and cybersecurity laws. As the 2017 *Verizon/Yahoo!* transaction demonstrates, the risk would be to acquire potentially significant liability for past infringements through the deal (Verizon paid US$350 million less for the acquisition following Yahoo!'s disclosure of two breaches affecting more than one billion accounts months after the initial purchase agreement). Even if the parties are not aware of a past data breach, the acquirer should investigate the security policies that the target has put in place to determine whether they are adequate or will require reinforcement when the deal closes. A prominent example of the risks in this regard was the 2014 acquisition of Viator, a tour booking company, by TripAdvisor. Viator experienced a cyberattack two weeks after the deal closed, resulting in notification of approximately 1.4 million customers that their personal information, including payment card data, might have been compromised and leading to a fall of 4 per cent in the value of TripAdvisor's stock. Finally, the acquirer should investigate what data security provisions are in place between the target and third parties. Contracts with data processors, including cloud service providers should be reviewed, but also more generally, agreements with other suppliers that give rise to data flows or create potential exposure for data security.

International M&A deals can involve the transfer of large amounts of personal data outside the EEA. Companies should make sure that they process such data in full compliance with the GDPR and its Belgian implementation. As discussed above, they must adopt appropriate protective instruments to transfer personal data outside the EEA, unless the country of the deal partner has obtained an adequacy decision from the EC.

Christian Duvernoy
christian.duvernoy@wilmerhale.com

Anne Vallery
anne.vallery@wilmerhale.com

Itsiq Benizri
itsiq.benizri@wilmerhale.com

WilmerHale
Brussels
www.wilmerhale.com

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

Good cybersecurity lawyers also understand the threats to IT security and how authorities expect companies to deal with them. They are not only GDPR experts, but they also understand the interaction between all EU cybersecurity instruments. Companies should look for lawyers who can communicate cybersecurity risk in business terms. Broad sector and geographic reach are also important assets.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

Advising in an area that is changing quickly but is of key strategic significance is challenging but fulfilling. This is also true of the many more specific interpretations of data protection law that will come in the next few years. Working in this area requires close monitoring of all developments as well as the ability to propose creative solutions. The EU cybersecurity framework is quite complex. A number of different legislative requirements may apply to the same company, particularly to providers of critical infrastructure and digital networks and services.

The interplay of EU competence and member state legislative and enforcement responsibility adds an additional layer of complexity. The NISD and the GDPR (even though it applies directly as a Regulation) both leave a significant amount of discretion to member states in how they will be applied.

How is the privacy landscape changing in your jurisdiction?

The NISD, the GDPR and the EECC are significantly changing the privacy and cybersecurity landscape in Europe. This new architecture is not only raising awareness, but it is also putting compliance with data protection and data security requirements at the core of the debate.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

According to ENISA's latest threat landscape report, the top five cyberthreats include malware, web-based attacks, web application attacks, phishing and denial of service.

Lexology GTDT Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes.

Led by WilmerHale, this *Privacy & Cybersecurity* volume features discussion and analysis of emerging trends and hot topics within key jurisdictions worldwide.

Market Intelligence offers readers a highly accessible take on the crucial issues of the day and an opportunity to discover more about the people behind the most significant cases and deals.

Covid-19 response
M&A risks
Latest regulatory trends
Cloud hosting

an LBR business

ISBN 978-1-83862-419-4