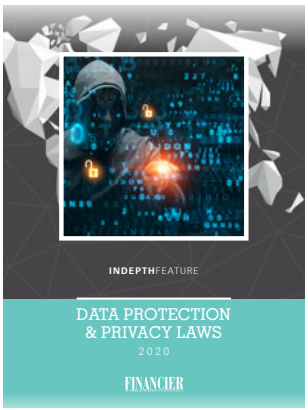

GIBSON DUNN

Published by Financier Worldwide Ltd

INDEPTH FEATURE Reprint November 2020

DATA PROTECTION & PRIVACY LAWS

Financier Worldwide canvasses the opinions of leading professionals around the world on the latest trends in data protection & privacy laws.

BELGIUM

Gibson Dunn

Respondents

ALEJANDRO GUERRERO
Of Counsel
Gibson Dunn
+32 2 554 72 18
aguerrero@gibsondunn.com

Alejandro Guerrero is a Spanish qualified of counsel in the Brussels office of Gibson, Dunn & Crutcher. Mr Guerrero advises on EU privacy and data protection rules, both at national level and from a US-EU standpoint. He is CIPP/E certified under the International Association of Privacy Professionals (IAPP) certification scheme for privacy professionals regarding European data privacy laws. He has assisted numerous clients in their GDPR compliance projects, including the review of their data processing activities, contractual arrangements and privacy policies, and has also represented clients in proceedings followed before authorities and courts in the EU.

SARAH WAZEN
Of Counsel
Gibson Dunn
+44 (0)20 7071 4203
swazen@gibsondunn.com

Sarah Wazen serves as of counsel in the London office of Gibson Dunn, where she focuses primarily on international arbitration, litigation and data privacy. Ms Wazen has extensive experience of international arbitration and cross-border litigation, with particular expertise in bilateral investment treaty arbitration. Ms Wazen regularly advises clients in relation to international and EU data privacy and cyber security matters, including complex cross-border investigations involving multiple regulatory authorities. Ms Wazen is a member of the International Association of Privacy Professionals (IAPP) and holds a CIPP/E certification.

Q. Do you believe companies fully understand their duties of confidentiality and data protection in an age of evolving privacy laws?

A: Companies have understood that the General Data Protection Regulation (GDPR) requires them to enhance their duties of confidentiality and data protection. For example, the GDPR introduced substantive obligations regarding security, confidentiality and accountability, which are clear to managers. Companies also understand that they need to minimise risks that could lead to reportable data breaches. However, companies may still need to fully comprehend and assimilate the practical implications of the GDPR. For example, data minimisation obligations require companies to ensure that only the requisite data is processed during the different stages of their operations. Thus, companies need to ask themselves whether they need all the data that they are collecting or processing at any given time to attain their objectives, and, if that data is needed, for how long it should be retained. Companies should also understand the benefits of applying pseudonymisation and purpose limitation protocols to limit undue data processing.

Q. As companies increase their data processing activities, including handling, storage and transfer, what regulatory, financial and reputational risks do they face in Belgium?

A: The Belgian Data Protection Authority (DPA) is particularly active against all kinds of companies, from big tech to European and Belgian companies that conduct more common data processing operations. The Belgian DPA is also active within the European institutional framework for data protection – the European Data Protection Board (EDPB) – and has already resorted to it in a number of cases. Data privacy is given considerable media attention in Belgium, so GDPR infringements can result in adverse publicity. For example, even for government-sponsored initiatives, such as the COVID-19 tracker application, the media and other stakeholders have spent significant time and resources explaining to the Belgian population the impact of this app. Finally, consumer associations and not-for-profit organisations have

The Belgian DPA is a committed authority that will not hesitate to act against GDPR violations, regardless of whether these affect large international companies or mechanisms used industry wide.

engaged in private actions and litigation in Belgium to safeguard the rights of data subjects, which can lead to significant financial and reputational risks.

Q. What penalties might arise for a company that breaches or violates data or privacy laws in Belgium?

A: Under the GDPR, all EU DPAs, including the Belgian DPA, can impose fines of up to €20m or 4 percent of the global turnover of a company. Notable fines imposed on companies include the €600,000 fine imposed on Google for a 'right to be forgotten' violation and a €50,000 fine imposed on a company for its failure to appoint a data protection officer (DPO). The Belgian DPA can also impose measures on data controllers that affect the manner in which they process data. For example, the Belgian DPA can order the rectification or erasure of personal data, or the restriction of processing of personal data. Lastly, the Belgian Privacy Act of 2018 foresees certain criminal sanctions for some GDPR infringements.

Gibson Dunn

Q. What insights can we draw from recent cases of note? What impact have these events had on the data protection landscape?

A: For a number of years, the Belgian DPA has taken an active role in terms of enforcement and advocacy. The Belgian DPA was one of the first EU DPAs to submit a consultation to the EDPB and to adopt a strong privacy stance in various cases covering numerous GDPR areas. The Belgian DPA has adopted fines on diverse matters, from privacy-sensitive issues such as the 'right to be forgotten' and the use of contacts to invite guests to online services, to formal violations, such as failures to appoint DPOs. In summary, the Belgian DPA is a committed authority that will not hesitate to act against GDPR violations, regardless of whether these affect large international companies or mechanisms used industry wide. Companies are expected to gradually ramp up their GDPR compliance levels as more decisions are adopted by the Belgian DPA and other relevant EU DPAs and EU courts.

Q. In your experience, what steps should a company take to prepare for a potential data security breach, such as developing response plans and understanding notification requirements?

A: Companies should first adopt preventive measures to prepare for potential data security breaches. These measures can comprise both technical and organisational measures that deter or hinder the materialisation of security threats. Companies should also implement measures that enable the early detection of data security breaches. For example, monitoring of traffic load, data extraction devices or code detection in outgoing emails can help identify the use of physical and digital means to unduly access and extract data. Finally, companies should put in place adequate response plans and policies, including the involvement of internal or external lawyers with access to the necessary notification requirements. Non-expert employees should be obliged to report violations as soon as they become aware, so that the response team can analyse possible security breaches and proceed to act as appropriate, within the legally established time frames.

Gibson Dunn

Q. What can companies do to manage internal risks and threats arising from the actions of rogue employees?

A: Companies can adopt measures to prevent, detect, report, remedy and hedge against actions of rogue employees. Whether it may be advisable for a company to adopt a lower or higher number of these possible measures depends on the specific activity or sector and the data processing operations at issue. Companies are increasingly turning to additional measures that allow them to fix or compensate any damage created by security breaches. However, remedial action can be costly in the context of data privacy and security violations, where companies may also incur penalties or fines. In some countries, both outside and within the EU, companies are increasingly turning to cyber insurance services for security and data privacy breach coverage. We expect Belgian companies to resort to these services more often.

Q. Would you say there is a strong culture of data protection developing in Belgium? Are companies proactively implementing appropriate controls and risk management processes?

A: This is generally the case among Belgian companies, which are broadly keen to comply with the GDPR in good faith. However, while controls and risk management processes may have moved in the right direction, this may not be sufficient to attain adequate levels of compliance with the GDPR. Companies are expected to gradually ramp up their GDPR compliance levels as more decisions are adopted by the Belgian DPA and other relevant EU DPAs and EU Courts. For example, the recent decision invalidating the EU-US Privacy Shield has led EU DPAs, including the Belgian DPA, to provide active guidance and direction to companies regarding cross-border transfers of personal data to the US. The ultimate objective is that companies embrace their GDPR obligations and objectives so that even violations by negligence can be avoided, and all kinds of data subjects, including consumers, users and employees, benefit from a privacy-safe environment in Belgium.❑

Gibson Dunn

www.gibsondunn.com

GIBSON DUNN represents clients across a wide range of privacy matters involving complex and rapidly evolving laws and regulatory requirements. The firm acts as a strategic partner, going beyond mere legal advice. Its privacy, cyber security and consumer protection team in EMEA includes lawyers with significant experience in compliance, litigation, government investigations, and corporate matters. The firm's clients seek its assistance on a broad variety of privacy issues, to benefit from pragmatic, sound reasoning and industry focus guidance. Gibson Dunn is also well known for handling strategic and high-profile privacy matters in the context of the development of cutting-edge technology.

ALEJANDRO GUERRERO Of Counsel
+32 2 554 72 18
aguerrero@gibsondunn.com

SARAH WAZEN Of Counsel
+44 (0)20 7071 4203
swazen@gibsondunn.com

GIBSON DUNN