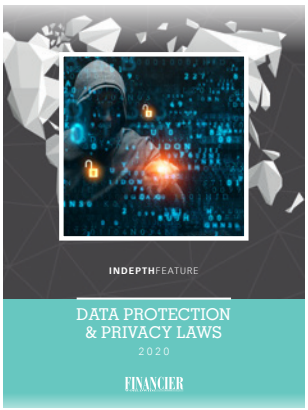

GIBSON DUNN

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.


FINANCIER
WORLDWIDE corporatefinanceintelligence

FRANCE

Gibson Dunn

Respondent

AHMED BALADI
Partner
Gibson Dunn
+33 (0) 1 56 43 13 00
abaladi@gibsondunn.com

Ahmed Baladi is a French qualified partner in the Paris office of Gibson, Dunn & Crutcher and the co-chair of the firm's privacy, cyber security and consumer protection practice group. His practice focuses on data privacy and cyber security, as well as technology and digital transactions.

REPRINT

Gibson Dunn

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

A: The General Data Protection Regulation (GDPR) has strongly contributed to the spread of data privacy compliance culture within organisations. Companies are increasingly aware of their obligations related to privacy and data security, which is a prerequisite to ensuring compliance. Yet, this is still a challenging task for companies to achieve for many reasons. First, EU member states still have the right to adopt additional requirements. Second, national supervisory authorities may have a different level of interpretation of certain provisions. Third, other non-EU countries have adopted data protection regulations that also need to be implemented, adding more complexity.

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

A: The French Data Protection Act (FDPA) reiterates the sanctions laid down in the GDPR – administrative fines of up to €20m or up to 4 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher. In addition, the FDPA provides for a wide range of sanctions that may be levied against a controller or a processor infringing their obligations, including a warning, the limitation or a ban of a processing and the suspension of data transfers. Moreover, a criminal sanction may be imposed in specific cases, such as five years imprisonment and a €300,000 fine or a €1.5m fine for a legal entity. Finally, a class action procedure is available for individuals to obtain compensation for moral or material damages. In all cases, it should be noted that the reputational risk for the sanctioned company may be significant.

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

Gibson Dunn

A: A significant ruling was issued by the French Data Protection Authority (CNIL) on Google LLC on 21 January 2019. Specifically, the CNIL imposed a €50m fine for breaches of EU transparency and information obligations and the lack of valid consent for targeted advertising purposes. With this decision, the CNIL became the first European data protection authority to levy significant sanctions against a major company, and it is still the highest fine issued under the GDPR to date. Considering this judicial precedent, businesses are taking privacy compliance more seriously as they are aware that the CNIL may take a strong position. Additionally, this decision highlights the importance of the 'one-stop-shop' mechanism, under which an organisation established in multiple EU member states will have, as its sole interlocutor, the supervisory authority of its 'main establishment', which is also known as the 'lead supervisory authority'. Indeed, if no lead supervisory has jurisdiction, such as in the Google case, any data protection authority may initiate an investigation against a company if it has not complied with the data protection requirements in the territory where such

Companies are increasingly aware of their obligations related to privacy and data security, which is a prerequisite to ensuring compliance. Yet, this is still a challenging task for companies to achieve for many reasons.

authority has jurisdiction. Complaints filed by associations or organisations against controllers constitute an additional source of concerns for many companies subject to the GDPR. The recent sanctions or investigations have, in many instances, been triggered by such complaints.

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: Preparing for a potential data security breach should not be limited to the incident response plan and notification obligations. It is even more critical to ensure that the company is up to date on its security measures, such as duly installing security patches, completing technology refreshes where required, auditing internal solutions and third-party providers, and anticipating or identifying technology vulnerability and end of life or obsolescence. In addition, the company should also have a comprehensive view of its ecosystem in order to mitigate any risk of a potential security incident expanding. Measures like back-ups, encryption and segregation seem a prerequisite of data to better manage a data security breach. Finally, the company should provide training to its employees on privacy and security to raise their awareness of security attacks, such as phishing emails.

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

A: Companies should have an IT charter in place in order to frame employees' access to and use of IT resources, such as the use of professional email accounts, internet access on the computer provided by the company and data protection measures. Control tools should also be implemented to monitor such use and identify any unusual activity from a rogue employee. From a general perspective, personal data should only be accessed by employees on a 'need-to-know' basis. Finally, as noted, the company should provide training to its employees on privacy and security to raise their awareness of external and internal security risks.

Gibson Dunn

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

A: Considering the financial and reputational risks, the active involvement of the CNIL through its enforcement actions and the increasingly high expectations of individuals, companies are increasingly implementing compliance programmes to address current privacy requirements and are even closely monitoring legal developments and case law to stay up to date with the evolution of the privacy landscape.❑

www.gibsondunn.com

GIBSON DUNN is known for excellence in the practice of law and is committed to providing the very highest quality of legal services. Representing its clients with passion and a drive to succeed, the firm combines a respect for tradition with a forward-looking emphasis on innovation. The firm is sought out for the exceptional creativity and problem-solving ability of its lawyers, who continually look for visionary solutions to its clients' legal issues. Gibson Dunn never gives ups, the firm originates novel approaches, makes headlines and changes the law.

AHMED BALADI Partner
+33 (0) 1 56 43 13 00
abaladi@gibsondunn.com

GIBSON DUNN