DE GAULLE FLEURANCE & ASSOCIÉS

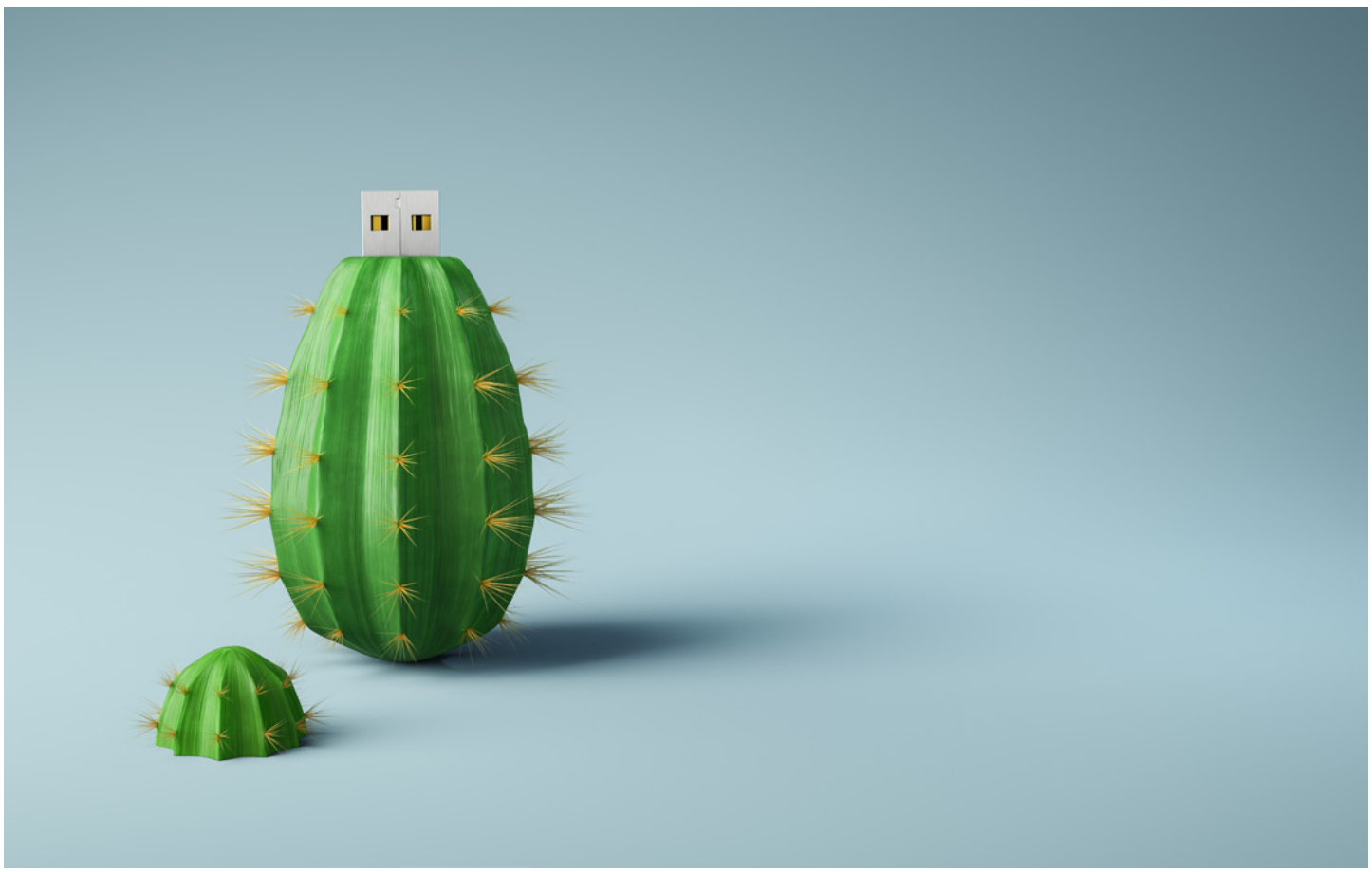
SOCIÉTÉ D'AVOCATS

Published by Financier Worldwide Ltd

INDEPTH FEATURE Reprint August 2021

DATA PROTECTION & PRIVACY LAWS

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



FRANCE

De Gaulle Fleurance & Associés

Respondents

CÉCILE THÉARD-JALLU
Partner
De Gaulle Fleurance & Associés
+33 6 61 92 05 29
ctheardjallu@dgfla.com

With a profile in IT, data protection, cyber security, blockchain, innovation technologies, commercial contracts and intellectual property law, Cécile Théard-Jallu has developed extensive experience in both the private and public sectors, particularly in the fields of health, environment, mobility, telecommunications and more generally the digital economy. She is certified to help businesses under the Europrivacy Horizon 2020-funded GDPR certification programme. She is listed in Best Lawyers 2021 in Information Technology Law and Biotechnology & Healthcare Practice, as a Leading Individual in Legal 500 EMEA 2020, and is ranked in Chambers 2021 in Industry Focus – Healthcare and Life Sciences.

NATALIIA IVANYTSKA
Associate
De Gaulle Fleurance & Associés
+33 7 72 07 81 67
nivanytska@dgfla.com

A member of the Paris and Kyiv Bars, Nataliia Ivanytska focuses on banking regulations, payments and the FinTech sector, financing transactions, international sanctions programmes and anti-corruption. She has extensive experience in assisting banks and other entities in the banking and finance sector to introduce FinTech solutions and payment schemes, and in negotiating partnership and commercial contracts. She also advises international groups on issues related to cross-border payments and acquisitions. She is also a guest speaker at the University of Paris 2 Panthéon-Assas in France.

De Gaulle Fleurance & Associés

Q. Based on your experience, do companies in France properly understand their data protection duties? To what extent are you seeing rising awareness?

A. Since May 2018, when the European Union's (EU's) General Data Protection Regulation (GDPR) became compulsory, French companies have gained a better understanding of their duties thanks to the efforts of the French Data Protection Authority (CNIL), new EU guidelines, experts involved in creating a compliance culture, the threat of a serious sanctions and the increasing risk of cyber attacks. In larger organisations, data protection officers (DPOs) have become more professionally trained and procedures have been put in place around a variety of topics, such as conducting privacy impact assessments or letting individuals exercise their data rights. Consumers are also more aware of the importance of data protection, which puts further pressure on data controllers and processors. However, many companies lack the means to be fully compliant or to maintain up to date practices. Also, several GDPR-related issues, such as data anonymisation and international data transfer, still lack sufficiently updated and harmonised guidelines, despite recent publications such as the new contractual tools recently adopted by the European Commission.

Q. When companies undertake data processing activities – including handling, storage and transfer – what regulatory, financial and reputational risks do they need to manage?

A. The GDPR has its own regulatory playing field, with a set of required technical and organisational risks management control obligations, as well as possible financial or operational sanctions directly impacting the activities of organisations. When they materialise, those risks impact both their internal and external reputation. When well mastered, they also allow parties to further secure and qualify sets of data, giving them a market advantage through the value that they can trigger. In the financial sector, the GDPR is part of a large, complex web of possibly interconnecting regulatory constraints, where risk control is a key activity of organisations. Data protection staff need to master and understand this whole framework. For instance, rules

De Gaulle Fleurance & Associés

Adequately securing data means adding value to the company's business and its internal and external reputation.

on anti-money laundering (AML) and countering the financing of terrorism (CFT) are particularly restrictive and may soon be reinforced. They require in-depth know your client (KYC) safeguards whose effectiveness depends on the combination of different personal databases. Therefore, the parallel enforcement of personal data protection principles is crucial, as the European Data Protection Board (EDPB) recalled in a letter of May 2021 to the European commissioner for financial services in charge of the EU AML-CFT framework reform. The fast developing cryptocurrency market is particularly watched in that respect. In the payment services market, the interplay between data protection and payment law rules also requires attention, as recalled in EDPB's Guidelines 06/2020 of December 2020.

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

A. Regarding sanctions, France is aligned with the principles of the GDPR. The CNIL has reinforced its control programmes and started issuing sanctions of up to several million euros, mainly

against large groups. France has become one of the EU countries which has levied the largest GDPR fines to date. In December 2020, an €800,000 fine was issued against Carrefour Banque, the banking subsidiary of the Carrefour Group, for failing to comply with GDPR and French rules on individual information, loyalty of data processing and cookies. Those administrative fines come on top of a regulatory landscape where criminal sanctions are becoming more common.

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

A. Data breaches often reveal a number of failings, such as insufficient levels of information being made available to data subjects, poor data backups, excessive or even unlimited data retention, inadequate choice of data processing legal basis or unlawful transfers of data to third parties. Most breaches are the result of internal negligence or failures to comply with IT security policies. This shows a need for reinforced training programmes for both employees and subcontractors, the use of secured standards, or investment in some certified IT tools. Some employers are also tightening their internal disciplinary rules in relation to data protection. This raises the issue of what means are made available to employees for their contribution to a better data protection environment and what can be reasonably expected from non-specialised employees operating in a socially and economically tense, increasingly digitalised and remote way of working.

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

A. All organisations, irrespective of their size and market share, should prepare for data breach episodes and must be able to react immediately. This means setting up both preventive programmes and crisis management plans, involving all levels within the organisation, including not only the IT team but also research and development (R&D), procurement, sales, communications, compliance and legal,

finance and the human resources (HR) departments. This also means involving the C-suite. From a legal perspective, all key issues should be anticipated and dealt with, including data protection, but also criminal, contractual, HR, regulatory, consumer, liability and insurance concerns. Mastering GDPR compliance, as well as cyber security regulations and the guidelines set forth by the French Agency for the Security of Information Systems (ANSSI), is key and often requires the assistance of external IT, insurance, crisis communication and legal experts. This particularly applies to actors in the financial services sector, where the processing of a huge volume of consumers' confidential personal data, or even sensitive data within the GDPR's purview, is at stake.

Q. What can companies do to manage internal risks and threats, such as rogue employees?

A. Companies can minimise threats by properly educating their employees to be more aware of data security risks, encouraging them to work with certified applications and respecting security procedures. IT charters or clauses in employment contracts stating that the employee shall abide by the company's internal regulations are also recommended and should be kept up to date. They may be reinforced by adequate digital tools, such as mobile apps or online bots which help employees to understand their data protection duties. Under certain conditions, disciplinary measures may also be enforced against rogue employees, possibly going up to dismissal.

Q. Going forward, how important will it be for companies to remain focused on data protection efforts, continually enhancing their controls and risk management processes?

A. Adequately securing data means adding value to the company's business and its internal and external reputation. This is progressively becoming a key criterion in the success of new commercial offers, compliance assessment programmes, fundraising projects or even to select candidates in tenders. For traditional banks, clients' databases constitute a great competitive advantage compared to emerging FinTechs. Actors within

De Gaulle Fleurance & Associés

the financial services sector should focus on opportunities offered by new GDPR compliance certification tools and bodies that will soon become available pursuant to articles 42 and 43 of the GDPR. Being pioneers in this domain will undoubtedly strengthen their position in the market similarly to what International Organization for Standardization (ISO) standards can bring, as this will help players identify and mitigate legal and financial risks and ensure a permanent legal watch. It will additionally offer reliable tools for international data transfers.❑

www.degaullefleurance.com

DE GAULLE FLEURANCE & ASSOCIÉS is a corporate full-service law firm assisting its clients in France and abroad with 180 people in the service of all clients and a relationship based on high standards, responsiveness and creativity. The firm has lawyers recommended in Chambers, The Legal 500 and Best Lawyers. The firm operates in 20 different languages (Arabic, Armenian, Chinese, Danish, Dutch, English, French, German, Hebrew, Hindi, Italian, Persian, Polish, Portuguese, Punjabi, Romanian, Russian, Tamil, Spanish, Ukrainian), and has lawyers registered in 13 Bars (England/Wales, Brussels, Beirut, California, Ireland, Israel, Kyiv, Luxembourg, New York, Paris, Quebec, Shanghai, Tunisia).

CÉCILE THÉARD-JALLU Partner
+33 6 61 92 05 29
ctheardjallu@dgfla.com

NATALIIA IVANYTSKA Associate
+33 7 72 07 81 67
nivanytska@dgfla.com

FRANÇOIS COUHADON Partner
+33 1 56 64 02 87
fcouhadon@dgfla.com

JÉRÔME LABROUSSE Partner
+33 1 56 64 00 10
jlabrousse@dgfla.com

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS