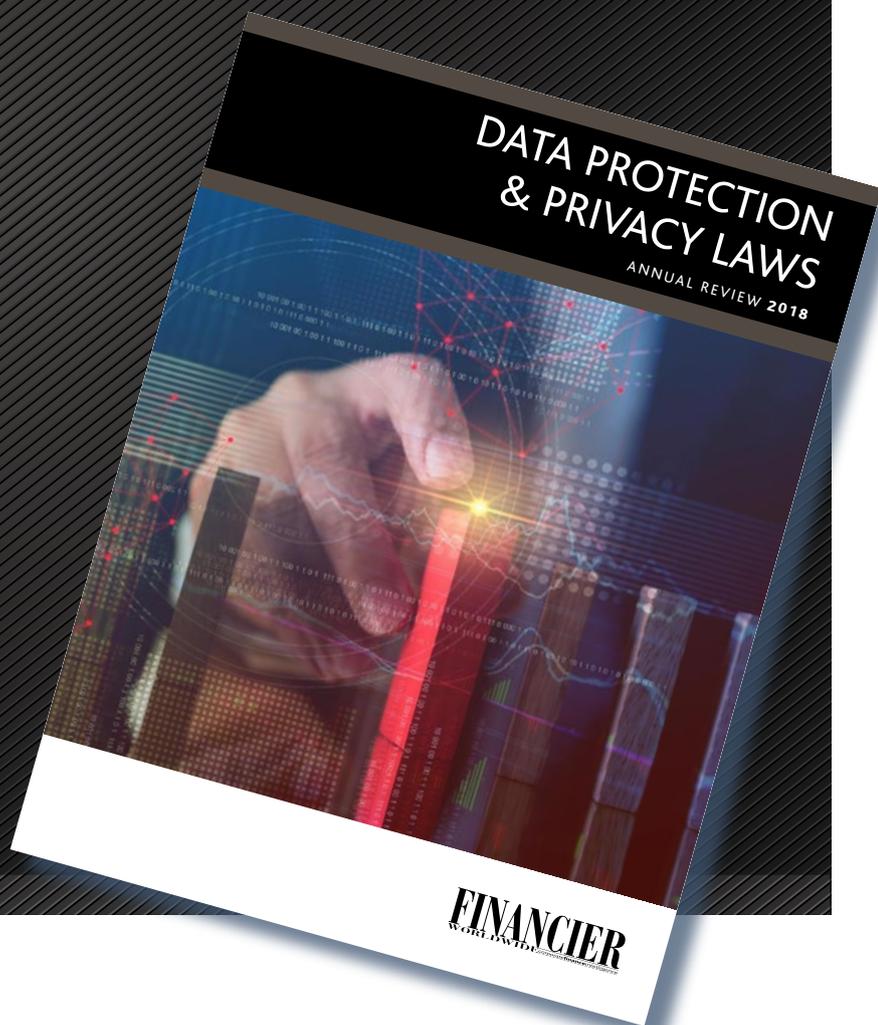


ANNUAL REVIEW

Data Protection & Privacy Laws

REPRINTED FROM
ONLINE CONTENT
DECEMBER 2018

© 2018 Financier Worldwide Limited
Permission to use this reprint has been granted
by the publisher



PREPARED ON BEHALF OF

**VOICU
FILIPESCU**
Attorneys at Law

FINANCIER
WORLDWIDE corporatefinanceintelligence



MARTA POPA
Voicu & Filipescu
Senior Partner
+40 21 314 02 00
marta.popa@vf.ro

Marta Popa has wide experience in various practice areas under Romanian law, including corporate consultancy, mergers and acquisitions, data protection matters, as well as project finance, public procurement, energy and employment law. She is a very experienced lawyer on data protection, advising international and local companies on all aspects of data protection law and practice, including GDPR end-to-end implementation and compliance projects, as well as GDPR audits. In the employment context, she was involved in compliance assessments regarding the use of employees' private data and advised on complex issues regarding the monitoring of their work activity.

Romania

■ **Q. In your experience, do companies in Romania need to do more to fully understand their data privacy and protection duties in the digital age?**

POPA: A first step toward General Data Protection Regulation (GDPR) compliance is a proper analysis of the internal business operations of a company, drawing up adequate and real data flows, followed by a proper GDPR gap analysis. Many Romanian companies, especially major but also small companies whose activity is data-sensitive, have made progress in complying with the GDPR which is, in part, due to Romania having highly skilled IT and security specialists who are involved in the process. There is still room for improvement until a significant number of local companies understand how the GDPR is impacting their business, which is a matter of management being aware of and educated about the impact and risks of digitalisation. For example, organisations are taking more of their data and applications to the cloud, thus increasing the risk of a cyber security incident, but are unaware of the related risks. However, the GDPR compliance rate remains low in Romania, with only 30 to 35 percent of companies achieving a satisfactory level of compliance. Given the benefit of having a skilled IT force, we believe that in the

years to come, organisations in Romania will become more and more educated and aware of the consequences of digitalisation.

■ **Q. Could you outline the latest legal and regulatory developments affecting corporate storage, handling and transfer of data in Romania?**

POPA: As of 31 July 2018, Romania adopted national measures for implementation of the GDPR through Law no. 190/2018. Law no. 190 establishes special rules on the processing of certain categories of personal data which take into account: genetic data, biometric data or health data, national identification number, personal data processing in the context of labour relations, personal data, and special categories of data in the context of performing a task that is of public interest. More specifically, with regard to the storage of data, Law no. 190 provides for special data processing conditions consisting of national identifiers, such as a personal identification number, identity card number and series, passport number, driving licence number or social health insurance number.

■ **Q. In what ways have the authorities increased their monitoring and enforcement activities with respect to data protection and privacy in recent years?**

POPA: The areas where most complaints were made, and increased monitoring and enforcement actions taken, related to processing of personal data in the context of credit checks at the credit bureau and video monitoring of electronic communications. However, such actions were insufficiently publicised in the media. In addition, the insignificant level of penalties applied – a maximum of €2000 – added to the lack of impact on companies. Generally speaking, while the data protection authority's profile in Romania was low until the GDPR's entry into force – except for 2017, when companies' preoccupation with conforming to the GDPR started to show in an increased number of data-related claims and data breach notifications 2018 has seen an increase in the profile and activity of the Romanian regulator. During 2018, Romania has adopted a series of national measures for implementing the GDPR, providing clarification of certain provisions, or derogations and exceptions where allowed under the GDPR.



■ **Q. What insights can we draw from recent high-profile data breaches? What impact have these situations had on the data protection landscape?**

POPA: Recent data breaches seem to have had the effect of ‘lessons learned’ for many companies. No organisation wants to find itself in the tough position of disclosing a data breach and protection of personal data seems to be paramount for companies which are processing this type of data. The consequences can be both immediate and long term, for the company as well as for its customers. Companies should learn that data breaches may damage the company’s value and reputation, and lead to potential regulatory fines, lawsuits and victim compensation. While it seems that individuals are more careful than ever about how their data is used by controllers, controllers themselves seem to be more aware of the risks of the increasingly advanced set of tools and techniques used to perpetrate breaches. We have seen an increased interest in Romanian companies compiling an adequate set of technical and organisational security measures to protect individuals’ data and a willingness to provide these to contractual partners when they conclude contracts involving data processing.

■ **Q. What steps can companies take to mitigate data risks arising from the use of third parties, such as consultants, agents and distributors?**

POPA: When using external service providers, companies should put in place a set of GDPR compliance audit control rules and procedures to check their compliance. The audit should cover

their data protection policies of their providers, employee confidentiality, management quality systems certifications and general technical and organisational measures.

■ **Q. What can companies do to manage internal data privacy risks and threats, such as liabilities arising from lost devices or the actions of rogue employees?**

POPA: The first measure would be to raise awareness of the existing business processes, data flows, vulnerabilities and associated risks affecting the rights and freedoms of individuals. Secondly, depending on the asset type, identified vulnerability and potential risk, different measures can be taken, such as changes to business processes, switching processors, encrypting for data in transit and at rest, asset and device management, and data classification and protection.

■ **Q. What essential advice can you offer to companies in Romania on managing data risk and maintaining regulatory compliance going forward?**

POPA: Companies should not rely on other companies’ experience or on policies or measures available from public sources. There is no ready-made or ‘one-size-fits-all’ solution. The best approach towards compliance with GDPR requirements is to take on board experienced GDPR specialists who can provide end-to-end conformance advice from a 360-degree perspective. In our view, the consultant team should include specialised lawyers, and specialised IT and cyber security specialists. Additionally, the compliance burden should not be placed on external consultants, but should

“ The best approach towards compliance with GDPR requirements is to take on board experienced GDPR specialists who can provide end-to-end conformance advice from a 360-degree perspective. ”

.....

actively involve staff members. As part of the initial compliance process, a company should implement training to ensure its internal team has been made aware of GDPR requirements. Going forward, once a satisfactory degree of compliance has been achieved with the help of GDPR specialists, a company must be aware that GDPR compliance is a continuous process. Among other measures, companies must refresh knowledge of GDPR requirements by providing

periodic training. Last, but not least, companies should engage with a good data protection officer (DPO) who can be consulted whenever a new business process in which personal data are used or new technologies are involved is initiated. ■

www.vf.ro

VOICU
FILIPESCU

Attorneys at Law

Since its establishment in 2001, Voicu & Filipescu has been one of the top Romanian law firms in terms of turnover, market position and reputation. Today the Voicu & Filipescu group include the law firm, a dedicated tax and accounting company and a specialised insolvency practice. In the data protection field, the firm offers expert advice to clients acting in various industries covering the full range of issues including GDPR compliance, data protection audits and trainings, data processing and transfer agreements, the preparation of PIA and DPIA, processing and the transfer of employee personal data, among others.

MARTA POPA
Senior Partner
+40 21 314 02 00
marta.popa@vf.ro

DANIEL VOICU
Managing Partner
+40 21 314 02 00
daniel.voicu@vf.ro