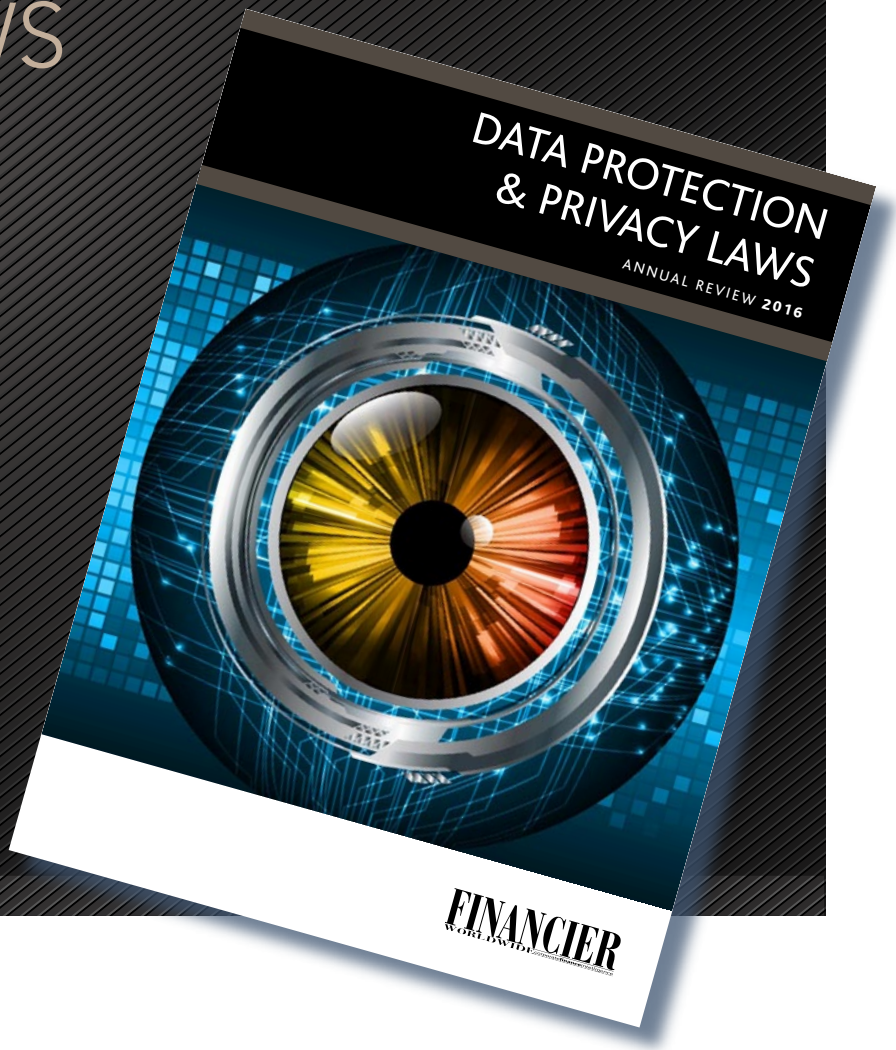
ANNUAL REVIEW

DATA PROTECTION & PRIVACY LAWS



REPRINTED FROM
ONLINE CONTENT
DECEMBER 2016

PREPARED ON BEHALF OF

Deloitte.

FINANCIER WORLDWIDE corporatefinanceintelligence

TURKEY

CÜNEYT KIRLAR
DELOITTE

Q IN YOUR EXPERIENCE, DO COMPANIES IN TURKEY PAY ENOUGH ATTENTION TO THE RISKS ASSOCIATED WITH DATA PROTECTION? ARE THEY BEGINNING TO FULLY UNDERSTAND THEIR DUTIES OF CONFIDENTIALITY AND PRIVACY IN THE DIGITAL AGE?

KIRLAR: The Turkish privacy law was published in the Turkish Official Gazette in April 2016 and entered into force at the same time, except for some provisions that followed six months later. As a consequence, the first phase of compliance with the law completed on October 2016. The law has been constituted in line with the relevant EU directive. Considering the enactment and publication of the new law of 'Protection of Personal Data Law', the maturity level of firms regarding compliance is still low. Discussions around the privacy law have continued for many years at a political and investor level, but various reasons have caused delay. The financial services and telecom industries are more aware of and ready to comply with the law than other industries, as they are already subject to specific regulations. Yet they still have a 'to-do list' in order to fully comply with the law. Besides, multinational firms and big conglomerates allocate necessary budget for their privacy investments in legal and IT consultancy and data protection technologies. A Data Protection Authority (DPA) that will strengthen and spread awareness of the law is underway and, once operational, it is expected that interest in privacy issues will increase.

Q COULD YOU OUTLINE THE LATEST LEGAL AND REGULATORY DEVELOPMENTS AFFECTING CORPORATE STORAGE, HANDLING AND TRANSFER OF DATA IN TURKEY?

KIRLAR: The privacy law draws a framework for processing personal data including collecting, inquiring, updating, sharing and using. Without obtaining explicit consent from the related person, personal data cannot be processed or transferred abroad or to third parties. The law clearly stipulates the circumstances when data can be processed without the consent of the related person. The processed data must be disposed after legally defined usage. Third parties receiving personal data, called 'data processors', have to take the necessary measures to provide the necessary security level. The data owner and the data processor have mutual responsibility to comply with the law. The data owner has the duty to perform periodical audits of the data processor to ensure a

consistent level of personal data protection. An important provision of the law is the one which clearly stipulates when processed data can be transferred to another country and when it can be transferred without the consent of the related person. The foreign country where personal data will be transferred should have an adequate level of protection and the countries where an adequate level of protection exists will be declared by the DPA.

Q IN WHAT WAYS HAVE THE AUTHORITIES INCREASED THEIR MONITORING AND ENFORCEMENT ACTIVITIES WITH RESPECT TO DATA PROTECTION AND PRIVACY IN RECENT YEARS?

KIRLAR: The DPA is authorised to monitor the performance of the law. The new Turkish privacy law imposes administrative fines and criminal sanctions for improper processing of personal data. The administrative fines vary from 5000 to 1m Turkish Lira. The administrative fine applies for non-compliance with the notification principle of individuals, non-compliance with security measures, non-compliance with DPA decisions and non-compliance with data controller registry articles. The imprisonment penalty varies from one to four and a half years and is referred to in the Turkish criminal code. The imprisonment penalty applies for recording personal or sensitive data related to religious beliefs, association and union membership, health information, sexual life, and biometric and genetic data, without obtaining explicit consent to do so or if such data is not disposed of at the end of the legal retention period. However, as the DPA is currently being established, there is no penalty that can be applied yet.

Q WHAT INSIGHTS CAN WE DRAW FROM RECENT HIGH-PROFILE DATA BREACHES? WHAT IMPACT HAVE THESE

KIRLAR: There are few publicly announced incidents in relation to data breaches in Turkey, but, according to the new privacy law, if any security breach occurs, the data owner must inform the data subject and the DPA immediately. The DPA can declare this personal data security breach from its website or any other appropriate channel. Therefore, we are

"Compliance with the new privacy law is a hot topic for firms in Turkey at present."

SITUATIONS HAD ON THE DATA PROTECTION LANDSCAPE?

anticipating that the reputational risk on data protection will be a top priority for boardroom agendas. Recent incidents have demonstrated that reducing data breach detection time and developing the ability to detect violations and anomalies are vital for effectively combating attacks.

Q THE USE OF THIRD PARTIES, SUCH AS CONSULTANTS, AGENTS AND DISTRIBUTERS, EXPOSES FIRMS TO UNIQUE DATA PROTECTION RISKS. WHAT ARE SOME OF THESE RISKS AND WHAT STEPS CAN BE TAKEN TO MITIGATE THEM?

KIRLAR: Third-party usage is an integral part of the value chain in business today and third-party risk should be delicately managed by firms in order to create value. Turkey's Banking Regulatory and Supervisory Authority regulates support services and defines the control framework that should be in place for the banking industry. There is no such specific regulation for other industries. The new Turkish privacy law defines the requirements for transferring personal data to third parties and the duties of the personal data processors. Contract management is essential for the effective management of the third party risk. Additionally, the confidentiality clause contract should include terms for transferring data protection responsibilities to third parties to ensure that the level of security controls determined by the law are put in place.

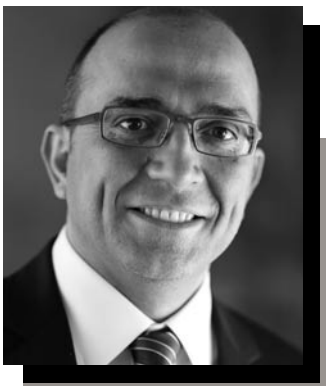
Q WHAT CAN COMPANIES DO TO MANAGE INTERNAL DATA PRIVACY RISKS AND THREATS, SUCH AS LIABILITIES ARISING FROM LOST DEVICES OR THE ACTIONS OF ROGUE EMPLOYEES?

KIRLAR: The human factor is an integral part of data privacy risk management. Moreover, employee awareness training of data privacy issues is crucial in combating the violations. Employees should be clearly informed as to their rights and responsibilities considering the new privacy law. Confidentiality and employment agreements need to include terms and conditions about privacy and should specifically state the conditions on the use of company devices, software and data. As well as employee awareness training, companies should also put in place automated controls in order to prevent the leakage of private data. After an inventory of data, a company can clearly decide what should be protected and implement technical solutions such as data leakage prevention, access control and encryption tools. The disk encryption method is a basic measure that can protect company data on lost devices.

Q WHAT ADVICE CAN YOU OFFER TO COMPANIES IN TURKEY ON MANAGING DATA RISK, INSTALLING INTERNAL COMPLIANCE PROCESSES AND MAINTAINING COMPLIANCE ON DATA PRIVACY GOING FORWARD?

KIRLAR: Compliance with the new privacy law is a hot topic for firms in Turkey at present. Although levels of compliance are not yet at the desired level, companies are building road maps and investing in processes, technologies and people. New sub-regulations are on the way and they will clarify compliance requirements in areas where they may be unclear. Companies should define their private data inventory, document their major data flows, identify key risks and then implement automated and manual controls to protect the data accordingly. An internal audit department should cover the privacy controls audit in their annual internal audit plans and give assurances regarding the compliance of privacy law to their board of directors. To create a sustainable privacy compliance programme, companies should adopt a privacy by design framework, which is based on proactively embedding privacy into the design and operation of IT systems, networked infrastructure and business practices.

Deloitte.



www.deloitte.com

Cüneyt Kırlar

Partner
Deloitte
+90 212 366 6350
ckirlar@deloitte.com

Cüneyt Kırlar is a risk advisory partner at Deloitte Turkey. With more than 23 years professional experience, Mr Kirlar has carried out many consulting and audit services related to information technologies (IT) management, IT risk management and compliance, information security and privacy and business continuity services. He has particular experience in the financial services, technology, media, telecommunications, manufacturing and consumer business industries. He also acts as the chief information systems auditor in the execution of independent information systems and banking processes audit where Deloitte provides audit services.

www.financierworldwide.com