The Guide to Data as a Critical Asset 2022 - Cybersecurity Compliance

11 Apr 2022

During the past decade, the regulation of cybersecurity has become a very hot topic in the world as a result of an increase in the level of importance attributed to data and privacy as well as the digitalisation of services, including government services. As the value of information systems and the data they contain increase, the security of these information systems and data becomes more and more important. Also, with the use of the internet of things (also known as IoT) in homes and workplaces, the cost of cybersecurity events has become more concrete and visible. Therefore, efforts to draw up a legal framework to ensure an adequate level of security have accelerated.

Data breaches are costly. During 2021, the average cost of data breaches rose from US$3.86 million to US$4.24 million.2 According to a report by Verizon,3 the financial impact of 95 per cent of a business email compromise is between US$250,000 and US$984,855, that of a computer data breach is between US$148,000 and US$1,594,648, and that of a ransomware attack is between US$69,000 and US$1,155,775. These figures do not take account of legal costs, liabilities and secondary costs, and on top of that is the associated loss of reputation and trust. According to research, companies that suffered a data breach were underperforming on the NASDAQ stock exchange after six months.4

Data breaches are also costly for data owners and data subjects. A data breach may lead to exposure of a person's private information. With the increase in the importance attributed to personal data, especially in the electronic environment created by the level of digitalisation and popularity of smart devices, there is now a new aspect of cybersecurity and the awareness for protection of data has entered a new phase. However, cybersecurity is not limited to protection of personal data, but has the purpose of protecting any data - or more accurately, the system and network as a whole. In this article, we examine the general framework for data security in the European Union and the United States to gain a better understanding of the latest trends. Then, as a more specific example, the current outlook in Turkey is explained.

Regulating cybersecurity

In the European Union, Directive (EU) 2016/1148 (the NIS Directive)5 was the first legal document setting out the regulation of cybersecurity across the Union. Being in the form of a directive, EU Member States have been able to adopt its requirements with a certain level of flexibility. Regulation (EU) 2019/8816 was enacted to complement the NIS Directive to establish a framework for cybersecurity certification. The NIS Directive requires Member States to ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks to the security of the network and information systems that they use in their operations. The term ‘operator of essential services' is defined as a public or private entity carrying out business in the field of energy, transport, banking, financial market infrastructure, health, drinking water supply and distribution, or digital infrastructure and that meet the following criteria:

- an entity providing a service that is essential for the maintenance of critical societal or economic activities;
- provision of the service depends on network and information systems; and
- an incident would have significant disruptive effects on the provision of that service.

The NIS Directive also requires Member States to adopt a national strategy on the security of network and information systems to define the strategic objectives and appropriate policy and regulatory measures.

As explained, the NIS Directive does not provide an EU-wide standard that applies to every and each entity, but instead requires the Member States to ensure the security of network and information systems in certain sectors by means of incident notification measures. A proposal presented to the European Commission on 16 December 2020 will repeal and replace the NIS Directive, and extends the scope to include new sectors such as telecommunications, social media platforms and public administration.

Most current legislation does not provide a sufficient standard for cybersecurity. To plug this gap, other frameworks and standards have been developed and published. In this respect, the European Union Agency for Cybersecurity (ENISA) has collaborated with the Standard Developing Organisations (namely ISO SC27, ETSI and CEN CENELEC).7

In the United States, there is no single legal document that determines a nationwide cybersecurity framework. However, the Health Insurance Portability and Accountability Act of 1996, the Gramm-Leach-Bliley Act of 1999 and the Federal Information Security Management Act, which is part of the 2002 Homeland Security Act, are the main pieces of legislation that set out certain cybersecurity requirements.

Under Executive Order 13636 on Improving Critical Infrastructure Cybersecurity, issued in February 2013, the National Institute of Standards and Technologies was assigned to develop a cybersecurity framework. Furthermore, the Cybersecurity and Infrastructure Security Agency has determined 16 critical infrastructure sectors that require an enhanced level of protection against cyberattacks, namely chemical, commercial facilities, communications, critical manufacturing, dams, defence industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation systems, and water and wastewater systems.

In addition, in 2014, the Securities and Exchange Commission's Examination Priorities included a focus on technology controls and cybersecurity. In Turkey, although cybersecurity is not an old concept, there is no specific law or regulation that governs cybersecurity standards. Nevertheless, since the enactment of the Personal Data Protection Law No. 6698 (the DP Law), cybersecurity has become an even more important concept for any data controller as data breaches can now lead to administrative fines as well as civil and criminal liability. The Personal Data Protection Board (the Board) has published guidelines regarding technical security measures to be taken by all data controllers, but this is limited to the protection of personal data. The DP Law introduced a new aspect to cybersecurity, namely that it is not limited to the protection of personal data but also the information system and network, including the data within it.

The minimum cybersecurity measures to be undertaken by public institutions and certain key sectors, such as telecommunications and banking, are also determined by a series of circulars and guidelines. Furthermore, cybersecurity standards adopted by the Turkish Armed Forces comply with the standards required by the North Atlantic Treaty Organization. There are also specific regulations for the protection of data in regulated sectors, including banking and capital markets.

In recent years, the establishment of the Digital Transformation Office of the Presidency of the Republic of Turkey (DTO) and National Cyber Incidents Response Center (NCIRC) were big steps towards establishing a more solid foundation for cybersecurity across Turkey. Both the NCIRC and the DTO publish guidelines regarding information security measures.

Following the steps taken by the European Union regarding cybersecurity, Turkey's Information and Communication Technologies Authority has initiated efforts to prepare a draft code regarding cybersecurity-related matters. This draft is expected to echo the NIS Directive and Regulation (EU) 2019/881 and establish a national cybersecurity standard. Additional legislation was planned as part of Turkey's National Cybersecurity Strategy for 2013-20148 and 2016-

2019,9 but no drafts have yet been published. Similar plans were included in the National Cybersecurity Strategy and the 2015-2016 Action Plan, but no draft has yet been made public. However, it was mentioned verbally by the Information and Communication Technologies Authority that work on cybersecurity legislation had been carried out.

Regulating cybersecurity with regard to the protection of personal data

Cybersecurity is a concept of security of information systems and the information they contain, regardless of the types of data. That being said, personal data protection regulation has made cybersecurity an important aspect of data protection regimes. In most jurisdictions, including Turkey, the most severe data breaches have been caused by a lack of cybersecurity measures. The scope of data protection regulations is limited to the protection of personal data; but as they require an adequate level of cybersecurity, they can be a guide for cybersecurity in jurisdictions where no specific universal cybersecurity regulation is in place.

Article 24 of Regulation (EU) 2016/679 (the General Data Protection Regulation (GDPR)) requires data controllers to implement appropriate technical and organisational measures to ensure their processing complies with the GDPR. Moreover, pursuant to Article 32, taking into account the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of variations in likelihood and severity for the rights and freedom of natural persons, data controllers and data processors must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, among other things:

- the pseudonymisation and encryption of personal data
- the ability to ensure continuing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability of and access to personal data in Turkey in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of data processing

Article 12 of Turkey's DP Law requires data controllers to take all necessary technical and administrative measures to provide a sufficient level of security to prevent unlawful processing, prevent unlawful access, and ensure the retention of personal data. However, the DP Law does not set out the minimum requirements for complying with this rule. The Turkish parliament, preferring to refrain from limiting the measures to be taken by data controllers, instead required data controllers to take all necessary measures to protect data, without any limitation.

Nevertheless, the Board has published a Guideline on Personal Data Security (Technical and Organisational Measures)10 (the DP Guideline) to guide data controllers on technical measures for the protection of personal data.

In the United States, the California Consumer Privacy Act allows any consumer whose non-encrypted and non-redacted personal information is subject to unauthorised access and exfiltration, theft or disclosure as a result of a business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect personal information, to institute a civil action for:

- recovery of damages in an amount not less than US$100 and not greater than US$750 per consumer per incident, or actual damages, whichever is greater;
- injunctive or declaratory relief; and
- any other relief the court deems proper

In summary, personal data protection regimes require a certain level of protection for systems that contain personal data.

Cybersecurity for public offices and critical infrastructure

The protection of state information systems as well as critical infrastructure has been regarded as a matter of national security for a while now. In fact, protection of critical infrastructure has been the main reason why several jurisdictions have adopted cybersecurity regulations. For instance, the NIS Directive and Regulation (EU) 2019/881 establish the protection of critical infrastructure. However, they do not include any requirements for information systems that are not considered as critical.

Turkey has adopted a similar path and regulates certain cybersecurity requirements to which public entities and critical infrastructure operators must adhere. A Presidential Circular on Information and Communication Security Measures,11 published in Official Gazette No. 30823 of 6 July 2019, governs security measures that should be taken by public institutions and operators providing critical infrastructure services so as to mitigate and eliminate the security risks faced in information systems and to secure the critical data that could jeopardise national security or cause destruction of public order when their privacy, integrity and accessibility have been compromised.

Sector-specific cybersecurity regulations

Owing to the importance attributed to their data, there are specific regulations regarding cybersecurity within the banking, insurance, e-commerce, telecommunications and health sectors. Apart from being considered as critical infrastructure, in many jurisdictions specific regulations have been adopted to protect the integrity and continuity of the information systems.

In Turkey for instance, the Regulation on Information Systems of Banks and Electronic Banking Services, published in Official Gazette No. 31069 of 15 March 2021, which is fully effective as of 1 January 2021, is the main legal document governing banks' information systems.12 This Regulation aims to regulate the minimum procedures and principles required as a basis for the management of information systems in the performance of banking activities, the provision of electronic banking services, and the management of the risks related thereto, and the information systems controls that must be established.

Electronic communications is another sector in which information systems are heavily regulated. In Turkey, the Regulation on Electronic Communication Infrastructure and Information System (the Infrastructure Regulation), the Network and Information Security Regulation in the Electronic Communications Industry (the Network Regulation) and Electronic Communication Law No. 5809 are the main pieces of legislation that govern the security of information systems of electronic communication institutions. The Infrastructure Regulation envisages the establishment of an Electronic Communication Infrastructure Information System in which the information regarding the infrastructure of operators within the electronic communication sector is recorded.

The Network Regulation regulates the procedures and principles to be followed by operators to ensure network and information security. The operators are obliged to establish an information system management system (ISMS), which is defined as all activities that are systematic, regulated, planned, manageable, sustainable, documented, accepted by the management of the operator, and based on international security standards (TS ISO/IEC 27001 or ISO/IEC 27001 standards), to ensure the confidentiality, integrity and accessibility of information. Operators must also implement an ISMS policy, an asset inventory and classification. The Network Regulation envisages certain security measures, including preparing risk management and evaluation, business continuity measures, management of information security breach and vulnerabilities, internal audits, employment, discipline procedures, physical access, protection against environmental threats, equipment security, electronic environment management, network security, separation of duties and environments, backing up, logging, user access management, password management, maintenance, and other measures.

The regime applicable to the health sector is relatively strict as regards processing of sensitive health data. The Regulation on Personal Health Data, Circular No. 2015/17 on Health Information Systems Applications and Information Security Policies Directive and Guideline are important legal documents that set out security measures to be adopted within the sector.

*This content was originally published in *The Guide to Data as a Critical Asset 2022 - Cybersecurity Compliance*.*

Related Practices

- Privacy and Data Protection

Related Attorneys

- BURCU TUZCU ERS?N, LL.M.
- BURCU GÜRAY
- CEYLAN NEC?PO?LU, Ph.D, LL.M.