KEEPING IT SAFE

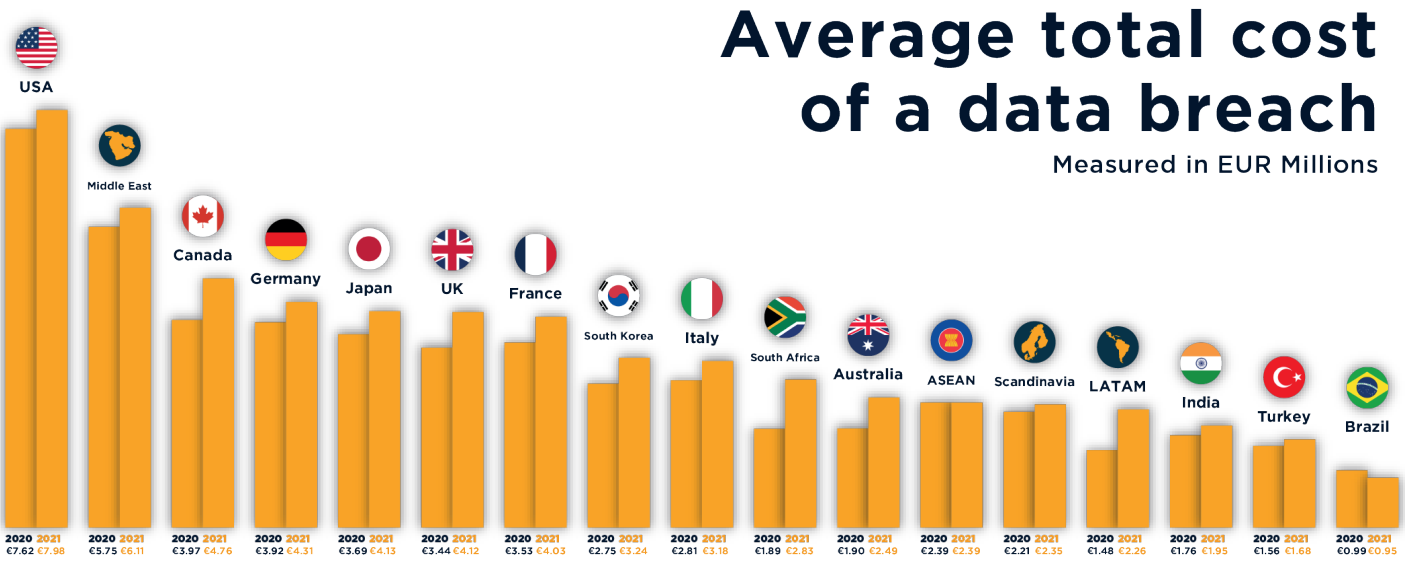
How Strategic European Union Partners Govern Sensitive Data

KAGENCY

INTRODUCTION

Introduction of the European Union's General Data Protection Regulation, known as GDPR, has increased the global interest in the standards that jurisdictions apply to the safeguarding of personal information. The emergence of big data as an immense opportunity for human prosperity also challenges the traditional frameworks of data collection and ownership. The modern tech organization manages an amount of personal information that far exceeds the information stored by governments - this is particularly true in developing nations.

2021 has been the year that we saw the highest increase in data breaches since 2015. Experts believe that this uptick can be explained by Covid-19 and the contact tracing apps that are introduced around the world without adequate infrastructure. Regardless of Covid-19, businesses are still very vulnerable to data breaches.



The aim of this research is to show and tackle the issues revolving around data security for companies in the Middle East. Around the world, 47% of businesses are victims of harmful or criminal cyber-attacks; it is not a number we can look past easily. More interestingly, this ratio jumps to 59% in the Middle East. A number that has an easy solution and countless copybook examples–in and outside the EU.

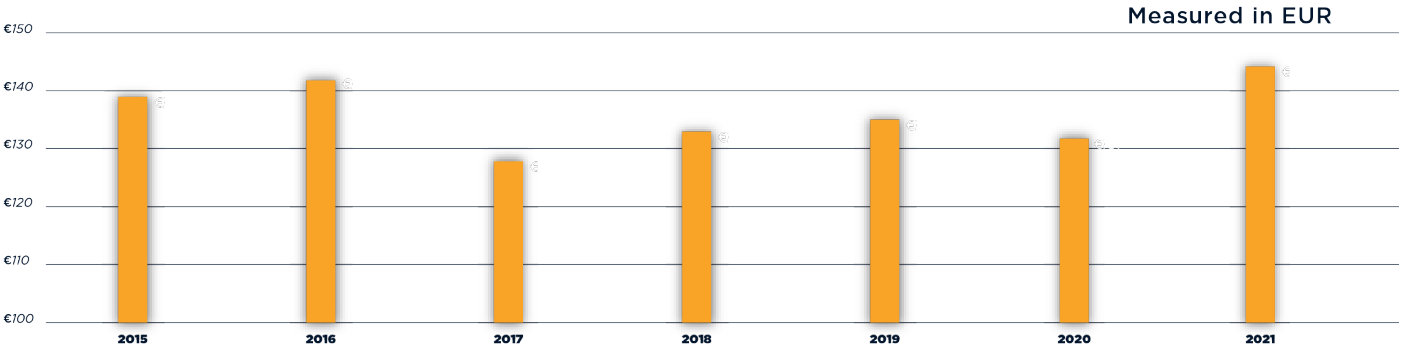
IBM has announced that 19% of data breaches in Middle Eastern companies are caused by human error, costing them $6.93 million[1]. Along with a higher rate of hacking in the Middle East, cyber-security seems like an obvious target for these companies to improve. Also, businesses also take longer to detect malicious and criminal attacks in the Middle East.

Data protection is a new issue, because it has been only a decade that com-

1 IBM Security, Cost of a Data Breach Report 2021, 2021.

panies have access to data on this level. It is a blessing and a curse: as much as our problems are still small (compared to what they can be in the future), every problem is new and unique. This requires us to be very much on top of the latest developments regarding data collection technologies and regulations, and always being open to new and effective solutions to tackle their shortcomings. Here, we aim to shed some light on to the existing rules and regulations in the countries bordering the EU, compare them and conclude with a set of recommendations for policymakers to implement their ideas effectively in different areas around the world.

Average per record cost of a data breach



This overview provides a detailed look into the legal frameworks that underpin data storage, transfer, ownership, access, information, and opt-ins and outs, applied to a variety of resources ranging from financial services to network providers and collection for security purposes. The countries in focus are Israel, Cyprus, Lebanon, Turkey, Georgia, and the United Arab Emirates.

On top of the existing legal structures, this document also takes a look at the liabilities involved, and the penalties imposed on entities and persons in the absence of adequately providing, storing, or managing data.

> *The General Data Protection Regulation (GDPR) has become a global standard for data collection and data privacy in recent years. As many strategic partners of the European Union shift their focus to data-driven businesses, it is crucial for these countries to adopt a data protection framework to enter the EU single market.*
>
> *Data sharing between the European Union and the EU's closest neighbors is not viable due to a lack of comprehensive data protection legislation. To boost the economy and become a part of the larger EU digital market, countries surrounding the EU including Turkey, Georgia, Lebanon, Israel, and the UAE, must implement a GDPR-based data privacy framework to foster economic relations.*
>
> *Implementing such a regulatory framework will boost the economy, inspire innovation, increase the available supply of goods and services, and create more opportunities for doing business between Europe and its closest neighbors.*

Luca Bertoletti

Director of Strategy at B&K Agency

ISRAEL

The Protection of Privacy Law governs data protection in Israel, which was implemented by the Privacy Protection Authority (PPA) in 2006. The legislation regulates the acquisition and use of personal and sensitive data, establishing the rights and obligations of those collecting and using the data, as well as security measures, and establishing the rights of those whose data is gathered and used.

1. GOVERNING TEXTS

In Israel, data protection is largely governed by the Protection of Privacy Law, 5741-1981, and the regulations promulgated pursuant to it, the Basic Law: Human Dignity and Liberty, 5752-1992, and the Privacy Protection Authoritys guidelines.

Additional legislation includes:

- Protection of Privacy (Data Security) Regulations, 5777-2017 (the Data Security Regulations)
- Amendment No. 40 to the Communications Law (Telecommunications and Broadcasting), 5742-1982 (the Anti-Spam Law)
- The Administrative Offenses Regulations (Administrative Fines and Protection of Privacy)
- Protection of Privacy Regulations (Transfer of Information to Databases Abroad), 5761-2001 (the Transfer of Information Regulations)
- Protection of Privacy Regulations (Conditions for Possessing and Protecting Data and Procedures for Transferring Data Between Public Bodies)
- Protection of Privacy Regulations (Conditions for Inspection of Data and Procedures for Appeal on a Denial of a Request to Inspect).

Although the PPAs guidelines do not have the force of law, they reflect the PPAs interpretation of the existing Privacy Law and should therefore be regarded.The guidelines include:

- 2/2011 Use of Outsourcing Services for Personal Data Processing
- 4/2012 Use of Security and Surveillance Cameras and Databases of Recorded Images
- 2/2017 Direct Mailing and Direct Mailing Services
- 5/2017 Use of Surveillance Cameras at the Workplace and in the Framework of Employment

- Draft Guidelines on the Transfer of Ownership in a Database which relate to database transfers in a merger & acquisition context
- 3/2018 Application of the Data Security Regulations to Organizations Certified Under ISO 27001.

2. SCOPE OF APPLICATION

The privacy law applies to all private, business, and public entities in Israel that possess or process personal information.

Additionally, the privacy law makes no specific reference to its jurisdiction and makes no requirement that the data subject be an Israeli resident or citizen. One could assume that the authority of the privacy legislation is confined to conduct occurring within Israel. The legal question of whether the privacy law applies to foreign entities processing personal information about Israelis and to Israeli entities processing personal information about non-Israelis is unresolved. However, suppose data transmission constraints are violated. In that instance, any further use of the data outside Israel will almost certainly be linked to the Israeli entity that breached the transfer limitations.

The law is applicable to and encompasses personal and sensitive data. As a result, while it is not obvious if it protects anonymous data, it is reasonable to presume that it does not.

3. DATA PROTECTION & REGULATORY AUTHORITY

The PPA, Israel's regulatory authority, was established in 2006 and is housed inside the Ministry of Justice.

The PPAs executive director is also the Registrar of Databases (the Registrar). The PPA is responsible for safeguarding any personally identifiable information stored in digital databases, including through administrative and criminal enforcement.

The PPA advocates for Israel's privacy rights on an international level and participates in the legislative process. As previously stated, the PPA issues recommendations that reflect the PPAs view of the privacy laws requirements. The PPA has investigative and administrative authority, and may perform inspections and audits of any entity subject to the privacy law. In some cases, the PPA may also impose administrative fines.

The Registrar is mandated to manage the Registry of Databases and is tasked with the responsibility of enforcing the privacy laws provisions and the regulations promulgated thereunder. The Registrar is authorized to deny registration of a database if there are reasonable grounds to believe that the database is being used or may be used for illegal activities or as a cover for such activities; or the data contained in the database was obtained, accrued, or collected in violation of the privacy law or any other law.

4. KEY DEFINITIONS

The privacy law regulates two principle matters: the general right to privacy and personal data protection in databases. The following terms are defined under the Israeli privacy law:

Personal data: data regarding the personality, personal status, intimate affairs, state of health, economic situation, professional qualifications, opinions, and beliefs of a person.

Sensitive data: Data on the personality, intimate affairs, state of health, economic situation, opinions, and beliefs of a person, and other information if designated as such by the Minister of Justice, with the approval of a parliamentary committee (no such determination has been made to-date).

A comparison between personal and sensitive data definitions reveals that sensitive data does not include data regarding a person's status and professional qualifications.

The data controller or *data processor*: The privacy law does not use the terms data controller and data processor but instead refers to database owner, database holder, and database manager.

Data security: protection of the data from disclosure, use, or copying performed without permission, or protection of the integrity of the data, i.e., that the data in the database is identical to the source from which they were extracted, and it has not been changed, delivered, or destroyed without permission.

Database: A collection of data, stored by magnetic or optical means and intended for computer processing, except for:

- a collection of data for personal use that is not business purposes; and
- a collection of data that includes only names, addresses, and contact information of persons, which in itself does not create any characterization that breaches the privacy of such persons, provided that neither the owner of the collection nor any corporation under its control has an additional collection of data.

Note that contrary to previous interpretations of this exemption, on 28 November 2018, the PPA clarified that a collection containing only names and email addresses would not fall under the exemption and, therefore, be considered a database.

Database holder: A legal person who permanently has a database in its possession and is permitted to use it.

Database owner: It is not defined in the privacy law. Some compare the role

of the database owner to that of the data controller under the EUs General Data Protection Regulation. Although there are several similarities, they are not the same. The privacy law does not generally state that the database owner is primarily responsible for complying with the privacy law.

Database manager: The active manager of the legal entity which owns or possesses a database or a legal person authorized to carry on such activities by the manager for this purpose.

Person: A natural person, as distinguished from a person for ownership of a database, which may be a corporation.

Biometric data: Data used to identify a person which is a unique physiological human characteristic that a computer can measure.

Health data: Data referring to a patient's physical or mental health, or data about his\her medical treatment. Not defined in the privacy law, but in the Patients Rights Law, 5756-1996

5. LEGAL BASES

A database owner who collects personal data directly from data subjects must obtain their consent and inform them of the following: whether they are required by law to supply the data, the purpose of the collection, and the identity and purpose of any third party who will receive the data.

Under the privacy law, no individual is liable for an act that he or she is legally empowered to perform.

6. PRINCIPLES

Confidentiality: A database manager, holder, or employee must not disclose any personal data except to carry out its duties, implementing the Privacy Law, or under a court order in connection with legal proceedings.

Storage Limitation: A database owner will annually review whether the data stored in the database exceeds what is required for database purposes.

7. CONTROLLER AND PROCESSOR OBLIGATIONS

The Data Security Regulations set a list of requirements regarding data security. These requirements must apply to a database owner, manager, and holder. Although the Data Security Regulations do not establish what specific technical information security measures a database owner must adopt, they do mandate the adoption of a series of corporate and managerial measures, as well as technological measures, that conform to the types of information that the organization stores and the uses that are made of the personal information. The security requirements may include, among other things:

- drafting a database settings document that will include a general description of the collection and processing of data and details of any transfer of data from the database to another country;
- development and implementation of an information security policy and procedures, that will include provisions as to the physical security of the site where the infrastructure of the database is located, access authorization to the database, and risks to which the database is vulnerable and how to resolve such risks, including by use of encryption mechanisms;
- taking reasonable measures, customary in employee sorting procedures, to verify that there is no concern that an employee should not be authorized to access the database;
- training and informing authorized employees of the requirements of the Privacy Law, the Data Security Regulations, and the security policy and procedures;
- limitation or absolute prevention of the possibility to connect a portable device to the systems of the database, considering the sensitivity of the data contained in the database;
- appointing an Information Security Officer (ISO);
- documenting any security incident;
- assessing the risks involved in the engagement with a contractor and regulating certain matters in a written agreement with the contractor;
- conducting a periodical review by a competent person, other than the ISO, to verify compliance with the provisions of the Data Security Regulations; and
- maintaining, securely, data accumulated in implementing the Data Security Regulations provisions for at least 24 months.

In the PPA guidelines regarding applying the Data Security Regulations to organizations certified under ISO 27001, the PPA outlined those organizations that are certified under and comply with ISO 27001 must be considered compliant with most of the requirements under the Data Security Regulations.

Subject to certain exceptions (see below), a database owner is required to register its database to the extent that one of the following conditions are met:

- the database contains data in respect of more than 10,000 data subjects;

- the database contains sensitive data;
- the database includes data about persons, and such was not provided by them, on their behalf, or with their consent;
- the database belongs to a public entity; or
- the database is used for direct mailing services.

A database must be registered before managing or holding the database unless the Registrar permits performing such acts before registration.

Although the privacy law imposes the obligation to register on the database owner, the privacy law also prohibits managing or holding a database that is required to be registered but has not been registered. Therefore, database managers or database holders could also face liability in connection with a database that is not registered.

Databases are exempt from the registration obligation where:

- the database only contains data made public according to lawful authority; or
- the database only collects data made available for public inspection according to legal authority.

The PPAs Transfer of Ownership Draft Guidelines presents its proposed position concerning the duties of database owners and the rights of data subjects in situations where the ownership of a database is transferred to another legal person due to the sale of the database or the merger or acquisition of the database owner. According to the Transfer of Ownership Draft Guidelines, such duties and rights include the following:

- the transferring database owner (the former owner) and the recipient database owner must notify the Registrar of such transfer of ownership;
- suppose the characteristics of the database recipient are different from those of the transferring database owner in a significant way that may adversely affect the rights of a data subject. In that case, the data subject's consent must be obtained before transferring the data to the database recipient. If such data subjects consent was not obtained, the data about them should not be transferred to the database recipient and should be erased;
- if due to the transfer of ownership in the database, the purposes of the processing of, or the processing activities performed on, the data in the database must change, the data subjects consent must be obtained before the transfer of the data to the

database recipient; and

- if, due to the transfer of ownership in the database, the purposes of processing and the processing activities must not change, generally notifying the data subjects of the transfer of ownership and contact details of the database recipient must suffice.

The Transfer of Information Regulations specify that data from an Israeli database may not be transmitted to another country unless the legislation of that country provides an equivalent level of protection for personal data to that afforded by Israeli law. On 1 July 2020, the PPA announced that its position is that the European Union's law ensures this level of protection, and thus that transfers of personal data to countries that are or were members of the European Union are permitted, provided that those countries continue to adhere to the European Union's personal data protection provisions.

On 1 July 2020, the PPA clarified that personal data may be transmitted to the United Kingdom following its exit from the European Union, as the United Kingdom is a signatory to Convention 108. This includes transfers to countries that have been granted adequacy status by the European Commission, as well as additional transfers to non-EU countries that comply with the GDPRs data transfer criteria.

If data is transferred, the database owner must receive a written commitment from the recipient that it will take sufficient security measures and will not transfer the data to any other person, whether in the same country as the recipient or not.

The Privacy Law requires database owners to create a database definitions document that includes the following information: a general description of the data collection and usage activities, the purposes for which the data is used, the types of data contained in the database, information about the databases overseas transfer, the database holders activities, the primary security risks and how they are addressed, and the database manager, holder, and ISO.

A database owner may be required to conduct a data security risk assessment in certain circumstances. Such risk assessment will be conducted at least once every 18 months.

A database owner must be required to appoint an ISO in certain circumstances. A data protection officer (DPO) appointment is not required under the Privacy Law. However, there is a requirement to appoint an ISO by an entity meeting one of the following conditions:

- entities holding five or more databases requiring registration;
- public bodies;
- banks, insurance companies, or companies involved in ranking or evaluating credit.

The database administrator must notify the Registrar of the ISOs identification. Failure to submit an ISO nomination when necessary may result in criminal penalties, as well as administrative fines. While the ISO is responsible for data security, the database owner, holder, and manager are each personally liable for data security under the Privacy Law.

The privacy law makes no requirement that the ISO be a citizen or resident of Israel. Anyone convicted of a crime involving moral turpitude or a violation of the Privacy Law is unable to serve as an ISO.

The Data Security Regulations provide greater information about the ISOs and database owners responsibilities. The ISO shall be funded by the database owner and shall report directly to the database manager. The ISO shall not execute any additional obligations that clash with its responsibilities as an ISO. The ISO shall create a data protection procedure, obtain approval from the database owner, and maintain the procedure on an ongoing basis. In certain instances, the database owner shall document and notify the PPA of any security occurrence.

A database owner is responsible for documenting any incident that raises concerns about the integrity of the data or any unauthorized use of the data. If a severe security event occurs, the database owner shall inform the PPA immediately and not later than 72 hours from its occurrence and report the steps taken following such an event. The PPA may order the database owner to inform the data subjects affected by the security event.

In addition to the general obligation to notify a security event, entities in certain sectors are subject to more specific legislation imposing additional duties.

Notably, the Ministry of Finances Supervisor of the Capital Market, Insurance, and Savings Authority (the Capital Market Supervisor) issued a circular covering financial institutions cyber risk management (such as insurance companies and investment banks). The circular requires financial institutions to report to the Capital Market Supervisor and to their Board of Directors any significant cyber event that results in the unavailability of systems containing sensitive data for more than three hours or if there is any indication that sensitive data has been accessed regarding financial institutions cyber risk management (such as insurance companies and investment banks). The circular requires financial institutions to notify the Capital Market Supervisor and their Board of Directors of any severe cyber event that results in the unavailability of systems containing sensitive data for more than three hours or any indication that sensitive data has been accessed.

A data subject may request that their personal information be deleted from a database. Under the Data Security Regulations, a database owner must determine each year if the amount of personal data in its databases exceeds what would be considered necessary for that database owner. Effectively, this necessitates the establishment of data retention regulations by database owners.

In its recommendations, the PPA stated that where a minor, or a data subject under the age of 18, is involved, the minor's parent or guardian must be informed and give informed consent to the collection and processing of personal data. Personal data on a child, a data subject under the age of 14, must be collected with the informed consent of the child's parent or guardian, and sensitive data about a minor, a data subject under the age of 18, must be collected with the informed consent of the child's parent or guardian.

8. DATA SUBJECT RIGHTS

Right to be informed: Upon collection of personal data from data subjects, a database owner must inform them: if they are under a legal duty to provide the data, the purpose of collection, and details of any third party that will receive the data and for what purpose.

Right to access: A database owner must either allow a data subject access to any data about them kept in the database or refuse to allow such access to the extent permitted by law.

A data subject may inspect any information about them that is kept in a database, whether in person or by a representative or guardian. The database owner must review the data in Hebrew, Arabic, or English, as requested by the data subject.

Suppose a database holder maintains a database on behalf of a database owner. In that case, the database owner must refer to a data subject asking to access the information from the database holder and instruct the database holder to allow such inspection.

According to the Data Inspection Regulations, the data subject must pay the owner or holder of the database a fee of ILS 20 (approx. €5,41) for the inspection. Inspection must be permitted within 30 days of the request, although the Registrar may extend the period by an additional 15 days.

The Data Inspection Regulations allow the database owner to provide a print-out of the requested information as the equivalent of permitting inspection of the data. Still, the print-out must not be removed from the premises of the database owner or holder without permission.

A database owner or holder may refuse the request for inspection of data from a database if:

- the database is of one of the types of databases the Privacy Law determines must not be subject to review (e.g., a database of security authority, tax authority, the database of the Israel Prison Service, data that the disclosure of may harm Israel's security or foreign relations or is prohibited by the provisions of any legislation); or
- The database is a service bureau that processes and stores data

for its customers, so long as the database owner or holder refers the data subject to the owner of the data on whose behalf the processing or storage services are performed.
- The data subject must be notified if their request to inspect data is refused within 21 days of the request, although the Registrar may extend the period by an additional 15 days.

If the request is denied, the data subject requesting the data may file a suit by the procedures outlined in the Data Inspection Regulations.

A database owner may refrain from providing data to a data subject for their inspection if:

- the data relates to the data subjects physical or mental health, and the database owner believes that such data may endanger the life of, or cause severe harm to the data subjects physical or mental health, then the database owner must provide the data to a physician or psychologist on behalf of the data subject; or
- it will breach a legal privilege applicable to the data, as prescribed under any legislation or ruling unless the data subject is the legal person for whose benefit the privilege is enacted.

Right to rectification: A database owner must respond to a data subject's request to rectify or erase any data about them kept in the database.

The Privacy Law provides that if a data subject inspects data about them and finds that it is inaccurate, incomplete, unclear, or not up to date, the data subject may request from the database owner or holder that such data be amended or deleted. This is, however, not an absolute right, and the database owner may refuse to accommodate such an erasure request.

Suppose the database owner agrees to the request. In that case, the amendments to the data or its erasure must be communicated to anyone who received the data from the database owner within the preceding three-year period. The data subject must be notified if their request to rectify or erase the data is refused within 30 days of the request, although the Registrar may extend the period by an additional 15 days.

A data subject may demand, in writing, from the owner of a database used for direct mailing that the information about him/her be deleted from such a database.

Right to object/opt-out: The Privacy Law allows a data subject to object to data processing only utilizing a civil suit based on the claim that the processing violates the data subject's right to privacy. However, there is no established concept of a general right to object processing once the personal data has been provided for processing without violation of privacy (e.g., with the data subject's consent). Today, it is generally understood that data sub-

jects in Israel do not have a right to withdraw their consent for processing.

In the PPAs Transfer of Ownership Draft Guidelines, a data subject's consent to processing must be obtained before transferring the data about such data subject to the new owner of the database.

A database holder and a database manager may be subject to administrative fines and civil and criminal liability.

9. PENALTIES

The Administrative Fine Regulations authorize the Registrar to impose administrative fines of ILS 2,000 (approx. €541) on an individual for:

- using, holding, or managing an unregistered database that requires registration;
- delivering false information in a database registration application;
- failing to deliver documents or an affidavit to the Registrar, on an annual basis, by a holder of at least five databases which require registration; and
- managing or possessing a database used for direct mail services without properly tracking the sources of the information used.

Administrative fines of ILS 3,000 (approx. €811) may be imposed for:

- managing or possessing a database used for direct mail services without designation of such use in the database registration;
- managing or possessing a database used for direct mail services without properly notifying data subjects or responding to requests for removal;
- failing to deliver information or delivering false information in a notice soliciting information that will be included or used in a database;
- failing to comply with data subjects inspection rights;
- granting access to a database to a legal person not authorized under a written agreement between the database holder and database owner; and
- failing to appoint an ISO for databases that are so required by law.

An administrative fine of ILS 5,000 (approx. €1351,84) may be imposed for using information from a database for purposes differing from those for which the database was registered.

A corporation must be fined fivefold for each of the aforementioned types of violations. For continuous violations, one-tenth of the fine may be levied for each day the violation continues after a warning has been served.

Those found guilty of the types of violations outlined above may face criminal culpability and a one-year prison sentence. These are strict liability offenses, which need no proof of criminal intent or negligence.

Those found in violation face a five-year prison sentence for disclosing data obtained through their position as an employee, manager, or holder of a database, except when disclosure is necessary to perform one's duties, to comply with the Privacy Law, or when disclosure is required by a court order in connection with legal proceedings. Violations of general privacy obligations, such as publishing or disclosing information obtained in violation of certain provisions of the Privacy Law, or publishing information about a data subject's intimate life or state of health, may result in a five-year prison sentence if committed with malice.

Under the privacy law, a breach of privacy is actionable as a civil wrong, and a claimant may seek monetary damages or an injunctive remedy. A court may pay damages of up to ILS 50,000 (about €13,519) for a breach of private rights without requiring proof of damages, and the damages may be quadrupled if the infringement was intentional. These statutory damages apply exclusively to individual claims and cannot be used to determine damages in a class action.

Along with establishing that a breach of privacy is a civil wrong, the Privacy Law provides that an act or omission in violation of some of its provisions may give rise to a tortious claim under the 2009 Torts Ordinance. This clause was inserted to ensure that even omissions, such as a failure to maintain data security, would constitute a civil wrong. Violations of privacy may be actionable as a class action under the Israeli Class Action Law in certain circumstances, such as business-consumer ties.

Notable cases of enforcement by the PPA:

- The PPA investigated and determined that two political parties (Likud and Yisrael Beiteinu) and a service provider (Elector Software) breached the Privacy Law due to a security incident that caused data concerning 6.5 million Israelis eligible to vote in the elections to be publicly available online.

The PPA explained that the political parties, as database owners, are responsible for compliance with the Privacy Law by the parties themselves and their service provider, a database holder. The PPA ceased the service providers operation until it had corrected the PPAs findings and implemented appropriate measures to protect personal data and sensitive data in its possession.

The PPA and the police investigated private investigators following complaints by data subjects regarding unauthorized access to personal data

about them held by insurance companies. The private investigators obtained certain personal data about the data subjects fraudulently and then used it to impersonate the data subjects and obtain sensitive data from the insurance companies. The investigation file was transferred to the prosecution for its review and determination.

- The PPA investigated a credit card company (Isracard) and determined that it breached the Data Security Regulations as a result of a security incident where an employee of the company stole a smartphone to which the company's customers sent all sorts of required documents via WhatsApp. In the aftermath, the company stopped the practice of using WhatsApp to send documents. The PPA determined that the company breached the Data Security Regulations by, inter alia, not limiting physical access to the smartphone and not using a password or fingerprint to limit technical access to the smartphone.

REPUBLIC OF CYPRUS

In Cyprus, data protection is primarily governed by the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), which has been transposed into Cypriot law by Law 125 of 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

1. GOVERNING TEXTS

The law, which took effect on 31 July 2018, adopted certain GDPR principles and repealed the 2001 Personal Data Processing (Protection of Individuals) Law.

To guarantee that the GDPR is applied properly, the Office of the Commissioner for Personal Data Protection has adopted certain guidelines published by the Article 29 Working Party, which has been superseded by the European Data Protection Board (EDPB), as well as its own guidelines and opinions.

The Guidelines from the Commissioner cover in particular:

- data protection officers
- Data Protection Impact Assessments
- personal data breach notifications
- codes of conduct and certification mechanisms
- security of processing
- data transfers
- records of processing activities
- health data retention
- video-surveillance
- employment relations
- use of the internet and mobile phones
- direct marketing of goods and services
- directions to banking institutions about retention periods for personal data
- directions for political communications through phone calls
- transmission of messages and placing of calls with political content/ promotion of candidates
- directions for the exercise of the right to access by public employees
- directions about retention periods for medical data
- Opinion 1/2018 addressed to Trade Unions in relation to the notification by the employers of lists with names of employees,

their salaries and contributions
- Opinion 2/2018 on video surveillance at work and the use of biometric systems
- Opinion 1/2019 on the access to email accounts of employee and former employee
- interpretation of Article 10 GDPR
- Opinion 1/2020 on the supervision of long distance/ online exams by higher education institutions
- Directive 4/2017 for right of access of employees or candidates in the Public Section.

In addition to the above Guidelines the Commissioner has also issued guidance in the form of public announcements, as follows:

- consent in the context of direct marketing (SMS and emails),
- announcement in relation to existing transmission licenses,
- sample of record of processing activities and directions for its completion.

Since the GDPR took effect in Cyprus, the Commissioner has investigated a number of incidents involving private entities and public agencies, for which public statements have been made. Reports produced throughout the year include summaries of the Commissioners decisions.

2. SCOPE OF APPLICATION

There is no national, territorial, nor material scope difference compared to the GDPR.

3. DATA PROTECTION & REGULATORY AUTHORITY

Cyprus's data protection regulating authority is the Office of the Commissioner, which was formed in 2002. Apart from the Commissioner, the office now employs nine officers and five administrative staff members.

The Commissioner is responsible for carrying out the duties and authorities delegated to them by the GDPR, the Law, and any other applicable regulation.

Subject to the provisions of Article 57 of the GDPR, and in addition to the duties provided for in that Article, the Commissioner carries out the following tasks (Article 24):

- publish on the Offices website the submission forms for com-

plaints and applications;

- examine complaints and, where possible, depending on the complaints nature and type, inform the complainant in writing of the progress and outcome of the complaint within 30 days of the submission of the complaint. If the complaint is deemed unfounded or does not fall within the responsibilities of the Commissioner, the Commissioner shall inform the complainant in writing within 30 days of the submission of the complaint;
- inform, where appropriate, the data subject, the controller, and processor of the time limits provided in Articles 60 to 66 of the GDPR;
- not examine complaints or discontinue its examination for reasons of public interest and must notify the data subject within a reasonable time of the reasons for the non-examination or the discontinuation of the examination of a complaint;
- draw up and publish the list of processing operations and cases requiring the appointment of a DPO, in accordance with the provisions of Article 14 of the Law; and
- publish on its website the list of controllers and processors available, who have appointed a DPO as provided for in Article 14 of the Law.

Furthermore, subject to the provisions of Article 58 of the GDPR, and in addition to powers provided for in that Article, the Commissioner exercises the following powers (Article 25):

- subject to the provisions of Article 58(1)(a) and 58(1)(e) of the GDPR, the Commissioner has access to all personal data and to all the information required for the performance of the duties and exercise of his/her powers, including confidential information, except for information covered by legal professional privilege;
- subject to the provisions of Article 58(1)(f) of the GDPR, the Commissioner may enter, without necessarily a prior warning of the controller, the processor, or their representative, any office, business premises, or means of transport, with the exception of private residences;
- for the exercise of the provisions of Article 58(a) of the GDPR and those of Article 25 of the Law, the Commissioner may be assisted by an expert and/or the Police; and during the exer-

cise of his or her investigative powers, the Commissioner may seize documents or electronic equipment under a search warrant, according to the provisions of the Criminal Procedure Law 1949.

4. KEY DEFINITIONS

Data controller: The natural or legal person, public authority, agency, or other body that determines, alone or in collaboration with others, the purposes and means of personal data processing; where the purposes and means of such processing are specified by Union or Member State law, the controller or specific criteria for its nomination may be specified by Union or Member State law.

Data processor: The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Personal data: Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to that natural persons physical, physiological, genetic, mental, economic, cultural, or social identity.

Health data: Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Biometric data: Personal data derived through particular technical processing of a natural person's physical, physiological, or behavioral traits that enable or confirm the natural person's unique identity.

Pseudonymisation: The processing of personal data in such a way that the personal data cannot be attributed to a specific data subject without the addition of additional information, provided that such additional information is kept separately and is subject to technical and organizational safeguards to prevent the personal data from being attributed to an identified or identifiable natural person.

5. LEGAL BASES

National provisions under Law 125(I) of 2018:

- When the offering of information society services directly to a child is based on the child's consent, the processing of personal data shall be lawful where the child is at least 14 years old.
- For a child younger than 14 years old, the processing of person-

al data referred to above shall be lawful when consent is given or authorized by the holder of parental responsibility over the child.

- The processing of genetic and biometric data for purposes of health and life insurance is prohibited.
- Without prejudice to Article 5, paragraph (1)(b) of the GDPR, where the processing of genetic and biometric data is based on a data subject's consent, the further processing of such data requires the separate consent of the data subject.

The processing of personal data vested in a public authority or body pursuant to a Council of Ministers Decision for the performance of a task carried out in the public interest or in the exercise of official authority shall be carried out lawfully and fairly, in a clear, precise, and transparent manner in relation to the data subject, in accordance with the GDPRs Article 5(1)(a) and Article 6(1)(e).

The combination of large-scale filing systems of two or more public authorities or bodies, is permitted only for reasons of public interest.

Personal data contained in official documents held by a public authority or organization for the purpose of carrying out a task in the public interest shall be released in accordance with the rules of the public sector law governing the right of access to records.

The processing of personal data by a controller or processor for the purposes of public interest archiving, scientific or historical research, or statistical purposes shall not be used to make a decision that has legal consequences for the data subject or has a comparably significant effect on them.

In Cyprus, the Electronic Communications and Postal Services Law 112 (I) of 2004 (the Electronic Communications Law) implements the Directive on Privacy and Electronic Communications (2002/58/EC) (as modified) (the ePrivacy Directive). Under the Electronic Communications Law, electronic mail may be used for direct marketing objectives only with the express consent of addressees.

In Cyprus, the only exception to the opt-out concept is when a sender receives an email address from a consumer within the course of a sale of goods or services. Individuals or legal entities that obtain personal data about their customers (e.g., e-mail addresses) during the sale of a product or service may use this data for direct marketing of their own similar products or services, as long as customers are made aware of this practice and given the option to opt out of future communications.

Archiving in the public interest, scientific, historical research, or statistical purposes: Processing carried out by a controller or processor for archiving purposes in the public interest, for scientific purposes, historical research, or

for statistical purposes excludes the use of personal data with the purpose of taking a decision, which produces legal effects vis-à-vis the data subject or significantly affects it in a similar way (Article 31 of the Law).

Processing genetic and biometric data for life insurance purposes: Processing of genetic and biometric data for life insurance purposes is forbidden under the Law. Notwithstanding the provisions of Article 5(1)(b) of the GDPR, when the processing of genetic and biometric data is based on the consent of the data subjects, separate consent of the data subject is required for the further processing of such data (Article 9 of the Law).

Journalistic, academic, artistic, or literary expression: The processing of personal data, special categories of personal data, or personal data relating to criminal convictions and offenses carried out for journalistic or academic purposes or for purposes of artistic or literary expression, is lawful, provided that those purposes are analogous to the intended objective and respect the essence of the rights as defined in the Charter of Fundamental Rights of the EU, in the European Convention of Human Rights and Fundamental Freedoms, which has been ratified by the European Convention for the Protection of Human Rights (Ratification) Law, and in Part II of the Constitution of Cyprus 1960 (Article 29(1) of the Law).

6. PRINCIPLES

Cyprus is totally committed to the GDPRs principles.

7. CONTROLLER AND PROCESSOR OBLIGATIONS

In the event that the GDPR requires the appointment of a DPO, the DPO should be notified to the Commissioner in writing or electronically (Article 14).

Any transfer of special category personal data to a third country requires prior notification to the Commissioner (Article 17).

Transfers of any special category personal data by a controller or processor to a third country or an international organization on the basis of the derogations allowed for in Article 49 of the GDPR for specified conditions require a DPIA and prior consultation with the Commissioner (Article 18).

Apart from the foregoing, communication with the Commissioner is needed where the controller restricts a data subject's rights or when the controller decides not to notify a data subject about a data breach (Articles 11(2) and 12(2)).

In the absence of a binding European Commission legal action, the Commissioner may propose to the Minister of Justice and Public Order the negotiation of agreements with third nations or international organizations for the

purpose of carrying out the GDPRs (Article 50 of the Law) aims.

Despite the provisions of Articles 46 and 47 of the GDPR, the Commissioner may, for compelling public interest grounds, place specific limitations on the controller or processors transfer of the aforementioned special categories of personal data.

Where adequate protections have been implemented by the Commission or in accordance with the consistency process set out in Article 63 of the GDPR, the Commissioner shall consult, before imposing the limits referred to above.

Additionally, notwithstanding the provisions of Article 49 of the GDPR requiring an impact assessment and prior consultation with the Commissioner, the Commissioner may impose explicit limitations on the controller or processors transfer of special categories of personal data for compelling public interest reasons.

An offense shall be committed by a controller or a processor who:

- does not maintain the record of processing activities provided for in Article 30 of the GDPR;
- does not update this record;
- does not make the record available to the Commissioner on request; or
- provides false, inaccurate, incomplete or misleading information to the Commissioner in relation to this record.

An impact assessment must be conducted when the processing is likely to create a high risk to the rights and freedoms of the persons concerned. Under the Law, the following activities require a DPIA and prior consultation with the Commissioner:

- measures to limit, in whole or in part, the rights referred to in Articles 12, 18, 19, and 20 of the GDPR (Article 11;
- exemption from the responsibility for data breach notification (Article 12);
- transfers of personal data to third countries or international organizations (Article 17);
- the combination of filing systems which concern special categories of personal data or data concerning criminal convictions or to be used with an identification card number or any other general application identity information (Article 10); and
- the enactment of laws or regulations pursuant to a law, which provide for a particular act or series of personal data process-

ing acts (Article 13).

A controller or processor's transfer of special categories of personal data to a third country or an international organization pursuant to Article 49 of the GDPR requires an impact assessment and prior consultation with the Commissioner.

The impact assessment referred to above shall include the information required by Article 35(7) of the GDPR, as well as a description of the technological and organizational security measures required by Articles 24, 25, 28, and 32 of the GDPR, as applicable.

The controller may be relieved, in whole or in part, of the obligation to notify the data subject of a personal data breach for one or more of the purposes set out in Article 23(1) of the GDPR.

Exemption from the obligation to notify data breaches requires a DPIA and communication with the Commissioner. The DPIA must include the information required by GDPR Articles 23(2) and 35(7). The Commissioner has the authority to impose requirements on the controller in exchange for the exemption (Article 12).

When offering information society services directly to a kid with the child's consent, it is permissible to process personal data if the child is at least 14 years old (Article 8(1)).

Processing personal data about a child under the age of 14 is permitted if consent is granted or approved by the person who has parental responsibility for the child (Article 8(2)).

The processing of specific categories of data set forth in Article 9 of the Regulation is permissible and legal when carried out for the purpose of publishing or issuing a court decision or when necessary for the purpose of delivering justice.

When a combination involves special categories of personal data, personal data relating to criminal convictions and offenses, or involves the use of an identity card number or another universally recognized identifier, a DPIA and prior consultation with the Commissioner are necessary. The impact assessment shall be conducted collaboratively by public authorities or entities intending to merge their file systems and shall include the information required by Article 35 of the GDPR.

8. DATA SUBJECT RIGHTS

Subject to the provisions of Article 23(1) of the GDPR, the controller may apply measures to limit, in whole or in part, the rights referred to in Articles 12, 18, 19 and 20 of the GDPR; provided that if the limitation of rights concerns a processing act entrusted to a processor, the measures shall apply subject

to Article 28 of the GDPR (Article 11(1)).

Right to be informed: The provisions of Article 14 of the GDPR shall apply to the extent that they do not affect the right to freedom of expression and information and press confidentiality (Article 29(2)).

Right to access: The provisions of Article 15 of the GDPR shall apply to the extent that they do not affect the right to freedom of expression and information and press confidentiality (Article 29(2)).

Right to erasure: For variations regarding the notification obligation regarding rectification or erasure of personal data or restriction of processing under Article 19 of the GDPR see section 8 above.

Right to data portability: For variations regarding the notification obligation regarding rectification or erasure of personal data or restriction of processing under Article 20 of the GDPR.

Authority powers: Subject to the provisions of Article 57 of the GDPR and in addition to the duties provided for in that Article, the Commissioner may not investigate a complaint or discontinue its investigation for reasons of public interest and shall notify to the data subject, within a reasonable period, regarding the reasons for not investigating or for terminating the investigation of the complaint.

9. PENALTIES

The Commissioner may impose administrative fines in accordance with the requirements of Article 83 of the GDPR. If the administrative fee is not paid, it is collected as a civil debt owed to the Republic. A fine levied on a public authority or public body for non-profit activity may not exceed €200,000. (Article 32).

Along with administrative fines, the Law establishes a number of criminal offenses for violations of specific provisions of the Law and the GDPR (i.e. Articles 30, 31, 33(1)(2), 34, 35(1), 42, Chapter V, and so on), which are punishable by imprisonment for one to five years and/or a fine ranging from €10,000 to €50,000, depending on the offense (Article 33).

If the controller or processor is a business undertaking or group of business undertakings, legal responsibility for deciding liability rests with the person designated as the undertaking or group of undertakings' highest executive instrument or body. If the controller or processor is a public authority or public body, the head or person responsible for the public authority or public body's effective management is legally responsible (Article 33(5)).

Notable decisions of the Commissioner under the GDPR to date include:

- A €5,000 fine, issued on 7 November 2018, against a public hospital for misplacement of a patient's file and refusal of a

subject access request.

- A €5,000 fine, issued on 12 April 2019, against a media organization for the processing of personal information without the data subject's consent. The case concerned the public broadcasting of the data subjects face in a video, regardless of the fact that anonymity was expressly requested.
- A €4,000 fine, issued on 13 March 2019, against an insurance company for sending unsolicited SMS marketing to non-customers, whose phone numbers were chosen randomly. You can read a summary of the decision in the February-April 2019 Report (only available in Greek, here).
- A number of fines ranging from €2,000 to €3,000, were issued against political parties and persons for unsolicited political messages for the European Parliament Elections.

THE LEBANESE REPUBLIC

Lebanon adopted Law No. 81 of 10 October 2018 on Electronic Transactions and Personal Data on that date. The law includes data protection requirements that are applicable in the Republic of Lebanon. Additionally, the Constitutional Council recognizes the right to privacy as a constitutional right.

MENA data security agencies - Founding years

Israel
adopted the law in
2006

Privacy Protection Authority
תנגהל תושרה תויטרפה

UAE
there is a cybercrime law adopted in
2012
but does not resemble a data protection law completely.

Cyprus
adopted the law in
2018

Cypriot Supervisory Authority

Georgia
adopted the law in
2011

The Office of the State Inspector

Turkey
adopted the law in
2016

Personal Data Protection Authority
KVKK

Lebanon
adopted the law in
2018

No agency

1. GOVERNING TEXTS

Prior to the law's implementation, Lebanon lacked precise laws governing the protection of personal data, and the legal landscape was defined by the absence of any statute addressing the subject of data protection. The law contains data protection measures in Title 5, titled "Protection of Personal Data."

This title is composed of the following chapters:

Chapter 1: General Provisions;
Chapter 2: Collection and processing of personal data;
Chapter 3: Required Procedure to enact the processing of personal data;
Chapter 4: The Right to access and rectify; and
Chapter 5: Criminal Provisions.

Articles 579 to 581 of the Code of Criminal Procedure provide sanctions in case of disclosure of professional secrets.

2. SCOPE OF APPLICATION

The law governs the processing of identifiable natural persons personal data. Additionally, the law establishes the rights of natural individuals whose data is handled (Article 1).

Additionally, the legislation establishes the responsibility of data controllers, which are individuals or legal entities that define the goals and methods of data processing (Article 1).

The territorial scope of the personal data protection provisions is not specified in the Law. However, Article 85 of the Law indicates that its rules apply to personal data processing conducted in the Republic of Lebanon. The Law expressly prohibits the application of any data protection provisions extra-territorially.

The Laws provisions apply to any automated or manual processing of personal data (Article 85). However, the rules of the Law do not apply to data processing relating to an individual's personal activities conducted for his or her sole personal benefit (Article 85).

Article 91 of the law establishes special categories for which data processing is banned, except within the narrowly defined scope. They include information about the data subjects health, genetic identity, and sex life.
It is worth noting that parties cannot agree to waive the application of provisions governing the rights of those affected by data processing or the responsibilities of those responsible for such processing (Article 85).

3. DATA PROTECTION & REGULATORY AUTHORITY

The Law makes no provision for the establishment of an impartial public authority to monitor the law's implementation. Lebanon, in fact, lacks an independent data protection authority.

Article 102 states that the data subject may bring a legal action before a local court to safeguard his or her right of access to and correction of gathered personal data, as well as to ensure the law's application.

It is worth noting that Article 95 requires the submission of a declaration to the Ministry of Economy and Trade (MoET) for the gathering and processing of personal data that is not exempt under Article 94.

In addition, Article 97 provides for the requirement of a special license delivered by the MoET for the collection and processing of personal data related to:

- foreign and national state security matters determined by a joint decision of the Ministry of National Defense (MoND) and the Ministry of Interior and Municipalities (MoIM);
- crimes and judicial cases determined by a decision of the Ministry of Justice (MoJ); and
- health issues, genetic identity, and sex life determined by the Ministry of Public Health (MoPH).

In Lebanon, there is no independent primary regulator for data protection. The MoET is authorized to receive declarations relating to the acquisition and processing of personal data that are not exempt under Article 94 of the Law (Article 95). Additionally, the MoET is empowered to provide a specific license for the gathering and processing of personal data as defined in Article 97.

4. KEY DEFINITIONS

Data controller: This means the natural or legal person who determines the purposes and means of the processing of personal data (Article 1).

Data processor: The law does not provide a definition of data processor.

Personal data: Any information related to a physical person which enables his/her identification, directly or indirectly, including by comparing information collected from various sources or by cross-checking various information (Article 1).

Sensitive data: The Law does not provide a definition of sensitive data. However, data related to the health, genetic identity, and sex life of an individual is subject to specific provisions (See Articles 91 and 97 of the Law).

Health data: The Law does not provide a definition of health data. However, data related to the health, genetic identity, and sex life of an individual is subject to specific provisions.

5. LEGAL BASES

Prior to the collection and processing of personal data, the Law does not require the controller to establish a legal basis. Rather than that, it requires data to be handled in accordance with several legal standards and gives data subjects a general right to examine and object to the processing of their personal data, subject to certain restrictions.

Article 91 of the law prohibits the processing of personal data related to the health issues, genetic identity, and sex life of the data. This prohibition is waived in the following cases:

- where the data subject has made the information publicly available or has explicitly consented to the processing of such data;
- where the collection and processing of such data are necessary to diagnose the data subject or administer treatment by a medical professional;
- where it necessary to prove or defend a right in court proceedings; and/or
- where the data controller has received authorization in accordance with Article 97 of the Law.

According to Article 87 of the Law, the data controller may not handle personal data for purposes other than those specified, unless the data processing is necessary for statistical, historical, or scientific reasons.

The Law has no definition of consent, no particular provision requiring consent for the processing of personal data, and no provisions defining consent conditions. Article 94 of the law exempts the data controller from the requirement to declare when the data subject consents to the gathering and processing of his or her personal data.

Article 92 of the law states that the data subject is not permitted to object to the collection and processing of his or her personal data if the data controller is required by law to collect such data or if the data subject consents to the collection and processing.

Article 94 of the Law exempts the following from the requirement to declare and/or obtain a license for the processing of personal data:

- by public legal entities;
- by a non-profit association; and
- for the purposes of updating records that aim to inform the public and that can be accessed by any person that has a legitimate interest.

6. PRINCIPLES

The principles of data protection mentioned in the Law are as follows:

- principle of purpose limitation (Article 87);
- principle of safe, lawful, specific, and transparent processing (Article 87);
- principle of accuracy (Article 87);
- principle of proportionality (Article);
- principle of storage limitation (Article 90);

- principle of security (Article 93); and
- principle of confidentiality (Article 106).

7. CONTROLLER AND PROCESSOR OBLIGATIONS

The Law imposes on the data controller the following legal obligations:

- the obligation to collect data safely and for legitimate, determined, and explicit purposes: Article 87 of the Law provides that personal data is to be collected safely and for legitimate, determined, and explicit purposes: the collected and processed personal data must be adequate and proportionate to the declared purposes. The personal data must be correct, complete, and up to date. The data controller cannot process personal data for purposes that do not coincide with the declared purposes unless the data processing relates to statistical, historical, or scientific purposes;
- the obligation to guarantee the safety of the collected personal data: Article 93 of the Law imposes an obligation to guarantee the safety, security, and integrity of the collected data;
- the obligation of declaration to the MoET: Article 95 of the Law imposes on the data controller an obligation to declare to the MoET the intent to collect and process personal data that is not covered by Article 94 of the Law; and
- the obligation to seek a license: Article 97 of the Law imposes on the data controller an obligation to seek a license from the MoET to collect and process personal data related to foreign and national state security matters determined by a joint decision of the MoND and the MoIM; crimes and judicial cases determined by a decision of the MoJ; and health issues, genetic identity, and sex life as determined by the MoPH.

Article 95 of the Law stipulates that prior to the collection and processing of personal data, a declaration must be given to the MoET. The format and content criteria for such a declaration are set forth in Article 96 of the Law. Additionally, Article 97 of the Law requires the issuance of a special license by the MoET for the gathering and processing of personal data relating to the following:

- foreign and national state security matters determined by a

joint decision of the MoND and the MoIM;
- crimes and judicial cases determined by a decision of the MoJ; and
- health issues, genetic identity, and sex life determined by the MoPH.

Article 94 of the Law exempts from the obligation of declaration and/or the obligation to seek a license for:

- the processing of personal data by public legal entities;
- the processing of personal data by a non-profit association;
- the processing of personal data for the purposes of updating records that aim to inform the public and that can be accessed by any person that has a legitimate interest;
- the processing of the personal data of students by education institutions for educational or administrative purposes;
- the processing of the personal data of employees or members of enterprises, commercial companies, associations, orders, and liberal professionals within the limit of the purposes of the professional activity;
- the processing of the personal data of customers and clients of enterprises, commercial companies, orders, associations, and liberal professionals within the limit of the purposes of their activity; and
- the processing of personal data of a data subject that has already given his/her explicit consent to the processing of his/her data.

Additionally, processing of personal data is excluded from the requirement to declare and/or get a license if it does not jeopardize private life or individual liberties.

Article 90 of the Law makes it illegal to retain personal data for a time longer than that specified in the declaration made to the MoET or in the decision authorizing data processing.

8. DATA SUBJECT RIGHTS

Right to privacy: The right to privacy is recognized by the Council as a constitutional right. It is also recognized by the following provisions which are considered an integral part of the Lebanese Constitution:

- Article 12 of the Universal Declaration of Human Rights;
- Article 17 of the International Covenant on Civil and Political Rights; and
- Article 16 of the Arab Charter on Human Rights;
- Professional secrecy in the Criminal Code.

Right to be informed: Article 88 of the Law imposes on the data controller an obligation to inform the data subject of the following:

- the identity of the data controller and his/her representative;
- the purposes of data processing;
- the mandatory or optional nature of the answers to the questions asked;
- the consequences of not answering the questions;
- the identity of the persons who will receive the personal data; and
- the right to access and rectify the collected data.

Additionally, and where data is not acquired directly from the data subject, the data controller must inform the data subject individually and explicitly of the data processing aims and his/her right to object to the processing. This obligation is waived if the data subject was aware of the data processing or if obtaining the data subject's information is difficult or requires excessive effort in comparison to the information utility (Article 89).

Article 99 of the Law confers to the data subject the right to request information related to:

- the purposes of the processing;
- the categories of processing;
- the sources of the processing;
- the subject of the processing;
- the nature of processing; and
- the identity of the persons that will receive the personal data or that have access to personal data as well as the purposes of this access.

Right to access: Article 99 of the Law confers to the data subject or any of his/her heirs a right to access the processed personal data. In addition, Article 103 of the Law restricts the right of the data subject to access personal data that was processed for the purposes of foreign and national security in case it endangers the foreign or national security of the State.

It should be noted that the data controller may refuse to comply with any abusive request made by the data subject or any of his/her heirs, especially in relation to their frequency (Article 100).

Right to rectification: Article 101 of the law confers to the data subject or any of his/her heirs a right to rectify, complete, and update the processed personal data. In case the processed data was sent to a third party, the data controller must inform the third party of the rectification.

Right to erasure: Article 101 of the law confers to the data subject or any of his/her heirs a right to the erasure of the processed personal data. In case the processed data was sent to a third party, the data controller must inform the third party of the erasure.

Right to object/opt-out: Article 86 of the Law provides that the data subject has the right to object to the processing of his/her personal data.

Article 92 of the Law grants the data subject the right to object to the collection and processing of his/her personal data, including the collection and processing of personal data for marketing purposes. However, the data subject is prevented from objecting to the collection and processing of his/her personal data in case the data controller is under a legal obligation to collect such data or the data subject has given his/her explicit consent to the processing of his/her personal data.

Right not to be subject to automated decision-making: The law does not contain a specific provision on the right not to be subject to automated decision-making. However, it is possible to infer such a right from the right to the object described above.

Other rights: Article 102 of the Law grants the data subject the right to bring legal action before local courts, particularly the judge of the urgent matter, to assure his or her right to access and rectify processed data, as well as to ensure compliance with the laws requirements.

9. PENALTIES

Article 106 of the law provides for a penalty of a fine of LBP 1 million (approx. €570) to LBP 3 million (approx. €1,700) and/or imprisonment of three months to three years for the following infractions:

- the processing of personal data without a declaration or a license;

- the processing of personal data in violation of the provisions of Chapter 2 of Part 5 of the Law; and/or
- the intentional or unintentional disclosure of processed personal data to unauthorized third parties.

Article 107 of the law imposes a fine ranging from LBP 1 million (approximately €570) to LBP 5 million (approximately €2,835) on any data controller who fails to comply with a data subjects request to access or rectify processed personal data within ten days or who does so in an insufficient manner.

According to Article 108 of the law, the sanctions set forth in Articles 106 and 107 of the law are aggravated in the event of recidivism. There are no recent decisions regarding the enforcement of the laws provisions.

REPUBLIC OF TURKEY

Turkey completed the final step in a lengthy process to enact the Law on Personal Data Protection No. 6698 in April 2016. (the Data Protection Law). The Data Protection Law was approved by the President and its full text was published on 7 April 2016 in the Official Gazette, Number 29677. Prior to this day, Turkey lacked particular legislation governing the protection of personal data.

From 7 April 2016, Turkey implemented a broad prohibition on the processing or storage of personal data without the data subject's explicit agreement, except to certain limited exceptions. Businesses that possessed personal data previous to 7 April 2016 were granted a two-year grace period during which they may ensure the data complied with the new regulatory requirements.

The process of enacting a local data protection law lasted more than 35 years, beginning with the implementation of the Convention on the Protection of Individuals with Regard to the Automatic Processing of Personal Data (Convention 108). Turkey signed Convention 108 on 28 January 1981 with the other Council of Europe member states but did not ratify it into national legislation until 2 May 2016, at which point it entered into force on 1 September 2016.

1. GOVERNING TEXTS

The Data Protection Law outlines a similar framework to the European data protection system within the framework of:

- Data Protection Directive (Directive 95/46/EC) (the Directive);
- General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR); and
- Data Protection Directive with Respect to Law Enforcement (Directive (EU) 2016/680).

In addition, secondary legislation in the form of regulations and communications further outline how Turkey's data protection regime operates in practice.

Key regulations include:

- Regulation on Deletion, Destruction, or Anonymisation of Personal Data 2017
- Regulation on the Data Controller Registry 2017
- Regulation on Working Procedures and Principles of the Personal Data Protection Board 2017

- Regulation on Organisation of the Personal Data Protection Authority 2018
- Regulation on Promoting and Change of Title of the Data Protection Authority Personnel 2018
- Regulation on Personal Data Protection Expertise 2018
- Regulation on Disciplinary Supervisors of Personal Data Protection Authority 2019
- Regulation on Personal Health Data 2019.

Key communiqués include:

- Communiqué on Principles and Procedures for Application to Data Controller 2018
- Communiqué on Procedures and Principles Regarding the Data Controller's Obligation to Inform Data Subjects 2018.

Additionally, the Personal Data Protection Authority (KVKK) clarified the minimal elements that must be included in an undertaking for cross-border transfers between a data exporter and a data importer located in another country.

Prior to the enactment of the Data Protection Law, data protection was governed by the Turkish Constitution, as well as general and sectoral legislation and regulations. These additional pieces of legislation continue to be valid in conjunction with the provisions of the Data Protection Law, as detailed below.

The Constitution makes no mention of data protection. However, the right to personal rights and privacy is enshrined in Article 20 of the Constitution, specifically in the section on Privacy and Private Life. As a result, everyone is guaranteed the constitutional right to:

- ask for protection of his/ her personal information;
- be informed of what personal data is held about them;
- access, delete, and/or correct such data; and
- be informed about whether the data is being used in accordance with the purpose for which consent was given.

Criminal Code Articles 134-140 declare unequivocally that criminal guilt is personal and so cannot be imputed to legal bodies. Nonetheless, a company's board of directors might be held accountable for privacy infractions. The criminal penalties that are contemplated in this regard vary from six months to four years. Additionally, as required by law, legal entities may be subject to safety precautions. As a result, the Criminal Code provides for the

following safety measures:

- privacy violations (Article 134);
- recording personal data (Article 135); and
- unlawful delivery or acquisition of data (Article 136)

Individual persons' rights are defined in Turkish Civil Law Articles 23 and 24. No one can waive his or her rights or capacity to act freely, even in the tiniest degree, under civil law. Neither can an individual waive his or her freedom, nor may anyone impose limits on an individual that are inconsistent with applicable laws and ethical standards.

Moreover, infringement of personal rights may constitute a tortious violation of privacy rights under the Turkish Code of Obligations.

The KVKK consistently publishes guidelines to clarify gray areas in practice as well as guidance on data protection matters in Turkey. KVKK has issued an English guideline on Data Protection in Turkey to create awareness for non-Turkish entities. In addition, various other guidelines on specific data protection-related matters have been published by KVKK on its website.

2. SCOPE OF APPLICATION

Article 2 of the Data Protection Law states the scope of the law. Accordingly, the Data Protection Law shall apply to:

- natural persons whose personal data are processed; and
- natural or legal persons who process such data fully or partially through automatic or non-automatic means only for the process which is part of any data registry system set out in the Law.

In this regard, the Data Protection Law protects personal data belonging to natural individuals and data pertaining to legal entities that are not covered by the Data Protection Law.

Before the law, there was no distinction between private corporations and state entities. As a result, the Data Protection Laws regulations and procedures apply to all institutions and organizations.

In contrast to the GDPR, the Data Protection Law has no territorial reach. That being said, in accordance with Turkish law's territorial principle, the Data Protection Law shall apply to all natural and legal persons processing Turkish-originated data, regardless of their location in or outside Turkey.

Personal data processing is defined as any operation performed on personal data, such as collection, recording, storage, retention, alteration, reorganiza-

tion, disclosure, transferring, taking over, making retrievable, classification, or preventing its use, fully or partially through automated or non-automatic means solely for the purpose of performing the process required by any data registry system. As a result, any system designed around a particular criterion for the purpose of facilitating access to personal data will be reviewed within the terms of the Data Protection Law.

The Data Protection Law foresees several exceptions under Article 28(1) where the Data Protection Law shall not apply:

- processing of personal data by natural persons within the scope of activities related to themselves or family members living together in the same dwelling provided that it is not to be disclosed to third parties and the data security obligations are to be complied with;
- processing of personal data for official statistics and research, planning, and statistical purposes after having been anonymized;
- processing of personal data for artistic, historical, literary, or scientific purposes or within the scope of freedom of expression, provided that national defense, national security, public security, public order, economic security, privacy, or personal rights are not violated or the processing shall not constitute a criminal offense;
- processing of personal data within the scope of preventive, protective, and intelligence activities carried out by public institutions and organizations duly authorized and assigned to maintain national defense, national security, public security, public order, or economic security; and
- processing of personal data by judicial authorities or execution authorities with regard to the investigation, prosecution, criminal proceedings, or execution proceedings.

In addition to the exclusions listed above, the Data Protection Law provides for partial exemptions in certain cases. Article 28(2) of the Data Protection Law provides that Article 10 concerning the data controllers obligation to inform, Article 11 concerning the data subjects rights, excluding the right to seek redress, and Article 16 concerning the requirement to register with the data controller registry system shall not apply in the following circumstances:

- is required for the prevention of a crime or criminal investigation;

- is carried out on the data which is made public by the data subject himself/herself;
- is required for the conduct of supervisory or regulatory duties, for disciplinary investigation, or prosecution by the public institutions, organizations, and professional associations having the status of public institutions assigned and authorized for such actions, in accordance with the power granted them by law; and
- is required for the protection of the States economic and financial interests with regard to budgetary, tax-related, and financial issues.

3. DATA PROTECTION & REGULATORY AUTHORITY

The Data Protection Law establishes two regulatory entities to ensure compliance with its provisions: the KVKK and the Data Protection Board. The KVKK is primarily responsible for administrative and government interactions, whilst the Board is the authority's decision-making institution.

The board began operating in January 2017, once all appointments were made. The board comprises nine members, elected as follows:

- five elected by the National Grand Assembly of Turkey; and
- four directly appointed by the Turkish president.

The KVKK was established as an independent regulatory authority with institutional and financial autonomy. It is responsible for ensuring personal data protection and raising awareness in this respect.

It is required that the board shall independently conduct and exercise the tasks and powers granted by the Data Protection Law and other legislation. Additionally, no organ, authority, office, or person has the jurisdiction to provide orders or instructions to the board about subjects within the scope of its duties and functions.

4. KEY DEFINITIONS

Data controller: means a real person or entity who determines the intended purposes and means of processing personal data. Data controllers are responsible for establishing and administering data registry systems.
Data processor: means a real person or entity processing data with the authorization of the data controller.

Personal data: includes any information relating to an identified or identifia-

ble natural person that can be used to identify that individual. For example, a customer's name and address, IP address, e-mail address, or a database of customer email addresses.

Sensitive data: special categories of personal data receive extra protection. This includes information that reveals the racial or ethnic origin, political opinions, religious or philosophical beliefs, appearance, memberships of unions, associations, or foundations, as well as information about health, sexual life, criminal records, or punitive measures, as well as biometric and genetic data.

Health data: means the health-related personal data (physical or mental) which constitute special categories of personal data, such as information about medical conditions.

Biometric data: means the personal data that uniquely identifies a person. Personal data is derived from technical processing relating to a real person's physical, physiological, or behavioral traits. For instance, photo, fingerprint, DNA, genetic characteristics.

Pseudonymization: is a technical and organizational measure by which personal data cannot be attributed to the data subject without any additional information. The related additional information is kept separately through an algorithm to ensure that the data subject cannot be attributed by using them.

Data Subject: (natural person concerned) means the natural person, whose personal data are processed. Under the Data Protection Law, real persons are the only beneficiaries of the Data Protection Law.

Explicit consent: means the consent which is based on the information and given with free will by the data subject. The Data Protection Law introduces a general prohibition on processing personal data or special categories of personal data without explicit consent. However, it does not envisage a specific method to obtain explicit content. In light of this, companies would be prudent to both record and retain consents, either in writing or electronically.

Processing activities: means any operation performed on personal data such as collection, recording, storage, retention, alteration, reorganization, disclosure, transferring, taking over, making retrievable, classification, or preventing the use thereof, fully, or partially through automatic means, or, provided that the process is part of a data registry system, through non-automatic means.

Data registry system: means the registry system which the personal data is registered into through being structured according to certain criteria.

5. LEGAL BASES

Personal data cannot be processed without the explicit consent of the data

subject where other legal bases are not applicable (Article 5(1)). Explicit consent should be freely given, specific, and informed (Article 3).

Personal data of each party to a contract may be processed by the other party provided that it is strictly necessary to execute or perform the contract, for example, processing personal information of an employee by an employer in order to execute an employment agreement (Article 5(2)(c)).

If explicitly provided for by law or it is necessary for compliance with a legal obligation to which the data controller is subject, personal data may be processed without the data subjects explicit consent. For example, preparing and holding personnel files by employers, collecting and reporting certain information by banks and financial institutions, and reporting personal information of a new employee to law enforcement agencies by employers.

Personal data can be processed in the protection of the life or physical integrity of a person, or of any other person who is bodily incapable of giving its consent, or whose consent would otherwise be deemed not legally valid. For example, location data of a mobile device carried by a missing person, or CCTV records can be processed for locating a missing person.

As per the Data Protection Law, the public interest is not a legal basis to process the personal data of a data subject without obtaining its explicit consent. However, the Board considers public interest as criteria while evaluating limits of independent press and the balance between the right to privacy and the right to freedom of expression.

Personal data may be processed without a data subject's explicit consent if such processing is necessary to the data controller's legitimate interests; provided, however, that processing does not harm the data subject's fundamental rights and freedoms (Article 5(2)(f) of the Data Protection Law). For example, the preamble of the Data Protection Law states that the owner of a company may process employee personal data to arrange job promotions, social rights, or in determining their role in the company's restructuring, each of which constitutes legitimate interests of the company.

As per Article 5 under the following conditions personal data can be processed without providing the explicit consent of the data subject:

- if the personal data is publicized by the data subjects themselves; and
- If it is mandatory for the establishment, exercise, or protection of certain rights.

6. PRINCIPLES

All data processing activities should be carried out in compliance with the principles for processing personal data (Article 4). The following key principles need to be adhered to for all personal data processing activities. Per-

sonal data must be:

- processed lawfully and fairly;
- accurate and where necessary kept up to date;
- processed for specified, explicit, and legitimate purposes;
- relevant, limited, and proportionate to the purposes for which they are processed; and
- retained for the period of time determined by the relevant legislation or the period deemed necessary for the purpose of the processing.

Data controllers are obliged to comply with data processing conditions while processing personal data. Personal data can be processed in cases where:

- the data subject has given his explicit consent;
- it is explicitly permitted by the laws;
- it is mandatory for the protection of life or to prevent the physical injury of a person, where such person is physically or legally incapable of providing his/her consent;
- processing of personal data belonging to the parties of a contract is necessary, provided that it is directly related to the execution or performance of that contract;
- it is mandatory for the data controller to fulfill its legal obligations;
- the personal data is publicized by the data subjects themselves;
- it is mandatory for the establishment, exercise, or protection of certain rights; or
- it is mandatory for the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the data subject are not compromised

7. CONTROLLER AND PROCESSOR OBLIGATIONS

Data controllers are obliged to (Article 12 of the Data Protection Law):

- prevent unlawful processing of personal data;
- prevent unlawful access to personal data; and
- ensure the retention of personal data.

The data controllers are responsible for implementing all required technical and organizational safeguards to ensure adequate data security. The Boards Personal Data Security Guide regarding technical and administrative measures published in January 2018 and the Digital Transformation Offices guideline for technical and administrative measures to be taken by public authorities and critical infrastructure organizations published in July 2020 can be used as references when complying with the data security obligation.

Unlike the GDPR, the Data Protection Law does not clearly govern the rights and obligations of the data processor, however there is still a need to maintain data security in collaboration with the data controllers. Within this framework, data processors must adhere to the data controllers instructions while processing personal data transferred to them and refrain from disclosing personal data they have learned. Additionally, they shall not use such data for any purpose other than the data controller's specified processing purpose. This obligation shall survive the termination of their role as data processor.

Other obligations:

- data controllers are obliged to carry out (or have third parties carry out) necessary audits to ensure compliance with the Data Protection Law within their own organization; and
- data controllers are obliged to comply with data transfer conditions for data transfers within Turkey and cross-border transfers.

The Board established that the data inventory must be kept up-to-date, accurate, and lawful. The registration process should be carried out in line with the data inventory and the changes in data inventory must be updated on the Data Registry System via VERBIS within seven days.

The data controllers must appoint a contact person who will be in charge of submitting data inventories and completing the registration process. Please note that the contact person must be a real person and a Turkish citizen residing in Turkey. In case that the data controller is located abroad, the data controller must appoint a data controller representative in addition to a contact person.

The Board held that the following categories of data controllers are exempt from having to register with the Registry:

- data controllers employing less than 50 employees and with an annual balance less than TRY 25 million (approx. €2,152,538) (unless the data controllers main business activity is processing special categories of personal data);
- data controllers processing personal data through non-auto-

matic means provided the processing is part of a data filing system;
- public notaries;
- associations (only for the personal data, processed in accordance with their area of activity);
- foundations;
- unions;
- political parties;
- lawyers;
- public accountants and sworn-in public accountants;
- customs brokers and authorized customs brokers; and
- mediators.

The Data Protection Law controls both domestic and foreign transfers of personal data. This is particularly true for international corporations and domestic businesses with operations extending outside Turkey's national borders. Businesses should perform an assessment of their operations to ascertain where personal data is stored and whether the new regulatory framework will apply.

The Data Protection Law requires explicit consent from data subjects for the transfer of personal data to third parties. However, consent is not required if the transfer is carried out in the following circumstances:

- expressly permitted under laws;
- necessary to protect the life or physical integrity of the data subject (or another person) where the data subject is physically or legally incapable of providing their consent;
- necessary to process data of the parties to a contract, if such processing is directly related to the execution or performance of the contract;
- necessary for the data controller to fulfill its legal obligations;
- already publicized by the individuals themselves;
- necessary to establish, use or protect a right; or
- necessary for the legitimate interests of the data controller, provided that such processing does not violate fundamental rights and freedoms.

In addition, the Data Protection Law stipulates that personal data on health and sexual life may only be transferred without explicit consent by persons under a confidentiality obligation, or by competent authorities, for the purposes of:

- protecting public health;
- operating preventive medicine;
- medical diagnosis;
- treatment and care services; or
- planning and managing health services and financing.

Consent will not be required for data transfers outside of Turkey where any of the exceptions above apply, and either adequate protection exists in the transferee country (the Board will announce the countries which it deems to have adequate protection, however until then, data controllers should consider that no country has such protection) or, where no adequate protection exists in the transferee country, the data controller has given a written security undertaking and the Board grants permission.

To determine the relationship between a data controller and data processor, the Board's decision dated 30 January 2020 and numbered 2020/71 can be taken as reference.

When granting permissions, the Board must evaluate international treaties, reciprocity of countries, measures taken by the data controller, as well as the period and purpose of the data processing. This requirement is particularly relevant for multinational companies and local companies, having cross-border operations or keeping data servers outside Turkey.

The Board can limit data transfers to third countries if it considers that a violation of public interest or personal interests exists. It is not clear how the Board will determine the criteria for such violation yet.

On 10 April 2020, KVKK announced Binding Corporate Rules (BCRs) allowing intra-group data transfers among multinational companies. BCRs are defined as data protection rules applicable for cross-border transfers that allow multinational group companies, operating in unsafe countries, to achieve an adequate level of data protection for the intra-group data transfers.

Due to the difficulties in the implementation of cross-border data transfer rules determined under the Data Protection Law, the KVKK was expected to issue new rules set for intra-group cross-border data transfers in parallel with the approach to BCRs accepted under the GDPR. Considering sector-specific needs, the KVKK introduced an alternative cross-border data transfer method specific to group companies, which is modeled after the EUs BCR approach.

BCRs, introduced by the KVKK, would allow multinational companies to transfer personal data from Turkey to a member of the same corporate group, located in a country with an inadequate level of data protection. BCRs are to be considered as a commitment to adequate data protection for intra-group cross-border data transfer in such circumstances.

BCRs must include all general data protection principles and adequate safe-

guards for protecting personal data in the corporate group. The KVKK gives a guideline on the necessary content of the BCR, as well as a standard application form on its official websites.

The Data Protection Law itself does not require the appointment of a data protection officer. That being said, the Data Controller Regulation, which includes the details of the registration process, requires data controllers located outside Turkey to appoint a data controller representative in Turkey to establish an account within the Registry. The representative can be either a legal entity, located in Turkey or a Turkish individual. The appointment of the representative must be made with a resolution of the data controller, which needs to be notarized and apostilled (or otherwise legalized).

Data controllers are obliged to notify the data subject and the Board within the shortest time, in case the processed data is collected by other parties through unlawful methods. Where necessary, the Board may announce such a breach on its official website or through other methods it deems appropriate.

The Board has published an announcement regarding COVID-19 (Coronavirus) on 23 March 2020. The announcement has specified that the Board will pay regard to the extraordinary conditions that data controllers are in with respect to the consideration of the periods that are necessary to be taken into account by data controllers in terms of complaints, notices, and data breach notifications submitted to the KVKK. As such, the KVKK envisages that the periods that data controllers are obliged to comply with may be evaluated taking into consideration the Coronavirus pandemic.

The Data Protection Law does not distinguish between the personal data of adults and minors. Personal data of adults and children are protected equally by the Data Protection Law though it contains no specific definition of a child. However, KVKK published a patch of guidelines regarding the matters which shall be considered in order to protect children's data. These guidelines are for consciousness-raising purposes on personal data concept, and they do not regulate any legal requirement regarding the processing of childrens data. It is expected to be introduced and to include specific provisions concerning the protection of children's data.

The Data Protection Law envisages specific rules for the processing of special categories of personal data that is defined as data relating to:

- race;
- ethnic origin;
- political beliefs;
- philosophical beliefs;
- religion, denomination, or other faiths;
- clothing and attire;
- membership of an association, charity or union;

- health;
- sexual life;
- criminal convictions and security measures; and
- biometric and genetic data.

Special categories of personal data can only be processed provided that the data subject has given his/her explicit consent (Article 6 of the Data Protection Law). In terms of additional legal bases for processing, the Data Protection Law divides special categories of personal data into two different categories:

- personal data related to health or sexual life; and
- other special categories of personal data.

While other types of special categories of personal data can be processed if such processing is permitted by the laws, personal data related to health or sexual life is protected more strictly than other special categories of data, as the scope of the legal grounds for processing is very limited. In addition to the requirement to obtain the explicit consent of the data subject, personal data related to health or sexual data can only be processed under the obligation of confidentiality, or by authorized institutions and establishments, for the purposes of:

- protection of public health;
- preventive medicine;
- medical diagnosis;
- provision of health care services and treatment; and
- planning and management of health care services and their financing.

8. DATA SUBJECT RIGHTS

Data subjects are entitled to request the following from the data controller (Article 11 of the Data Protection Law):

- information about whether their personal data has been processed;
- if personal data has been processed, the information about such data and processing;
- information about the purpose for the data processing and whether the data was used for this purpose;
- information about the identities of natural or legal persons

whom the data is transferred;
- correction, erasure, or removal of the personal data;
- if data is transferred, the data controller advises the recipient about correction, erasure, and removal of the personal data;
- objection to any negative consequence of their data is analyzed exclusively through automated systems; and
- compensation where a data subject suffers any damage due to the illegal processing of their data.

Right to be informed: Regardless of the legal basis of data processing, data controllers are obliged to inform the data subjects when collecting personal data in respect of the minimum mandatory content outlined below (Article 10 of the Data Protection Law):

- the identity of the data controller and its representative, if any;
- the purpose of personal data processing;
- the recipients to whom the personal data can be transferred, and the purpose of the transfer;
- the methods and legal reasons of collection of personal data; and
- the data subject's rights under Article 11 of the Data Protection Law.

Right to access: Data subjects are entitled to request the following from the data controller (Article 11):

- information about whether their personal data has been processed;
- if personal data has been processed, the information about such data and processing;
- information about the purpose for the data processing and whether the data was used for this purpose;
- information about the identities of natural or legal persons whom the data is transferred;
- correction, erasure, or removal of the personal data;
- if data is transferred, the data controller advises the recipient about correction, erasure, and removal of the personal data;
- objection to any negative consequence of their data is analyzed exclusively through automated systems; and
- compensation where a data subject suffers any damage due to

the illegal processing of their data.

The KVKK has issued the Application Communiqué which regulates the methods and procedures to lodge a request with data controllers. Accordingly, data controllers should respond to requests duly lodged by data subjects within 30 days. The Application Communiqué also provides for a processing fee of TRY 1 (approx. €0.1)for each page which may be charged for responses exceeding ten pages, or the cost of the data recording medium (if the answer is given in this manner).

Right to rectification: In accordance with the principles of lawful data processing activity, personal data is only processed when it is accurate and kept up to date. In line with such principle, data subjects are entitled to request for rectification from the data controllers, in case of contrary practice.

Right to erasure: Data controllers are obliged to erase, destruct, or anonymize the personal data ex officio or upon the demand of the data subject, in the event that the reasons for which it was processed are no longer valid (Article 7).

The details of the erasure, destruction and anonymization process are governed by the DDA Regulation. In addition, a Guide on Erasure, Destruction, or Anonymisation of Personal Data has been prepared by the Board, in order to clarify the implementation in this respect. It should also be mentioned that data controllers which are required to be registered with the Registry must draft a data storage and extermination policy. The mandatory content of the policy has been envisaged under the aforementioned regulation. Data controllers are obliged to publish their policy/procedures related to data retention and extermination.

Right to object/opt-out: The Data Protection Law does not provide a general right to object to data subjects. In case of the existence of a legal basis for data processing, the right to object will not be sufficient to cease processing activities. However, in case of the legal basis purpose excess, the data subject may use its right to object in order to cease processing activities which are exceeding the purpose of legal basis such as legitimate interest. In addition to that, the data subjects may always have the option to revoke their consent and stop the data processing which is being carried out based on the explicit consent of the data subject.

In addition to the above-stated perspective of the Data Protection Law, there is alternative legislation regulating the right to object/opt-out of the data subjects within electronic commerce practice. The Electronic Commerce Law No. 6563 states that personal data collected from a consumer can only be used and shared with third parties with the consumer's consent. Therefore, the consent of the data subject, that is in the consumer's position, must be obtained in order to use their personal data for marketing purposes.

Right to data portability: Unlike the GDPR, the Data Protection Law does not provide the right to portability to data subjects. Under the Data Protection Law, data subjects are not entitled to have their personal data transmitted

directly from one controller to another.

Right not to be subject to automated decision-making: The Data Protection Law does not grant a general right not to be subject to automated decision-making systems. The processing limits and rights of the data subjects shall be evaluated by considering the other legal requirements under Data Protection Law such as the purpose of the legal basis etc. However, based on Article 11(1)(g) of the Data Protection Law, data subjects have the right to object to any negative consequence of their data being analyzed exclusively through automated systems. Please note that such rights can be used by the data subjects in the presence of a negative consequence. The existence of an automated decision making system is not enough to use such a right, but it is necessary to have negative consequences against the data subject created by the system.

9. PENALTIES

Certain breaches of data protection law can result in imprisonment under Turkish law:

- prison sentences (ranging from six months to four years) or judicial fines can apply for unlawful collection, processing, and transfer of personal data under the Criminal Code;
- safety measures may be imposed on legal entities such as cancelation of licenses or seizure of the goods used for or gained as a result of the commissioned crime or benefits gained from the commissioned crime determined under Article 60 of the Criminal Code;
- administrative fines ranging between TRY 5,000 (approx. €324) and TRY 1 million (approx. €65,000) will apply for breaches of the Data Protection Law;
- individuals can claim compensation for unlawful collection or processing of personal data; and
- sector-specific regulations also contemplate administrative fines, see for example the Regulation on Administrative Sanctions of Information and Communications Authority, which imposes fines on authorized operators (service providers, network providers, infrastructure operators) worth up to 3% of the preceding calendar year's net sales for violating personal data and security obligations.

The Board published six principle-decisions stating the main principles which shall be taken into consideration by the data controllers. The details of such

principle decisions are mentioned below under board decisions. Such principle-decisions underlines the following criteria;

- all data processing activities must comply with the conditions under Articles 5 and Article 6 of the Data Protection Law for processing personal data, and persons processing personal data must also comply with other requirements under the Law;
- the entities providing services at service counters, box-offices and desks must ensure that only authorized persons are in these locations, as well as take necessary measures to prevent people receiving services at these locations from seeing or hearing each other's personal data;
- the data controllers must take all necessary technical and organizational measures to provide appropriate data security in order to cease and prevent unauthorized accesses and misuse of the authority;
- advertising, using data subjects contact details unlawfully should cease;
- individuals and organizations use software programs, which allow them to question personal data, through data which obtained in various ways are unlawful and such usages are subject to procedural actions under Turkish Criminal Law; and
- reasonable measures should be taken to verify the contact information declared by the data subjects via sending a verification code and/or link to the phone number and/or e-mail address, etc.

Board decisions

Principle decisions published by the Board include:

- Decision Number 2018/63 on the unauthorized access and usage of the data: the Board announced that the data controllers must take all necessary technical and organizational measures to provide appropriate data security in order to cease and prevent unauthorized accesses and misuse of the authority.
- Decision Number 2018/119 on advertising using data subjects contact addresses unlawfully: the Board announced that advertising using data subjects contact details unlawfully should

cease. The Board stated that those advertising via email, SMS, and calls should also cease such activities and the Board will impose sanctions for failures to do so.

- Decision Number 2019/308 on individuals and institutions using various software programs that allow questioning personal data: the Board determined that individuals and organizations use software programs, which allow them to question personal data, through data obtained in various ways. The Board specifically referred to attorneys, law firms, individuals, and organizations operating in the finance, real estate, and insurance sectors. The Board announced that the use of such software programs is not in not in compliance with Article 12 of the Data Protection Law and the data processors using such software programs shall be subject to procedural actions under Turkish Criminal Law.

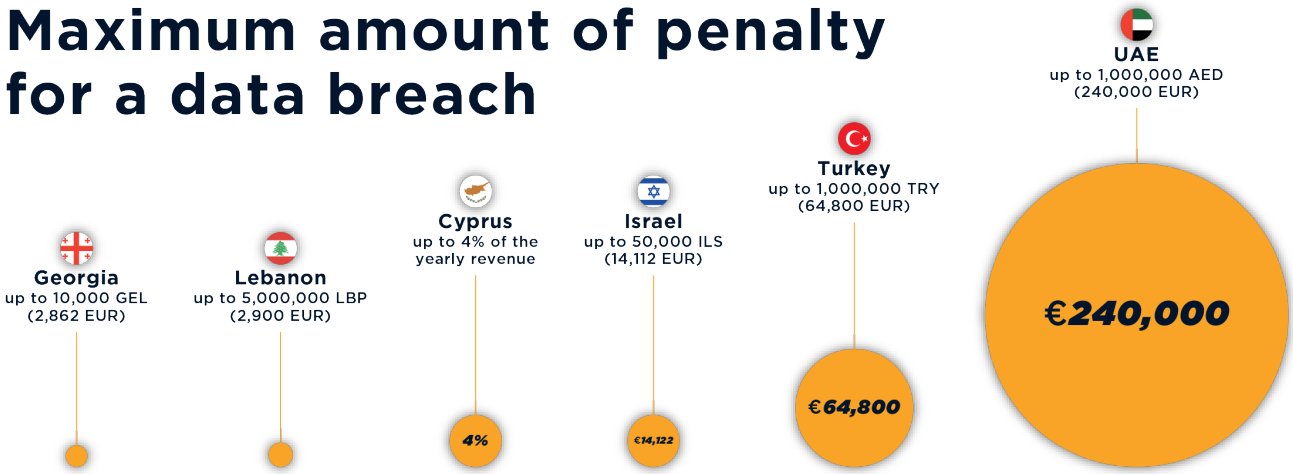
The KVKK has also published the Board's summarized and anonymized decisions to help to clarify legislation and practices in this developing area, giving some insight on how the Board will treat certain aspects of data processing, transfers, and security breaches. Notable points from the decisions include:

- Decision Number 2020/481 on the right to be forgotten: The Board stated that the search engines, operating based on the data collected from third-party websites are data controllers, carrying out data processing activities. The Board evaluated the delisting requests of the data subjects from search engines as a subtitle of the right to be forgotten. To consider such requests, a balance test between the data subject's fundamental rights and freedoms and the public's interest in obtaining the information is required. The Board published a list consisting of 13 criteria, which may be used while making such a balance test.
- the Board refused a data subject's request to remove his/her name from a column in a journal, on the basis that freedom of press overrides their right to privacy.
- the Board announced that Microsoft notified the Board on 8 May 2019 due to a data breach that occurred in the company system. Microsoft instructed that the ID information of a customer support manager working for one of its service providers

has been unauthorisedly obtained by third parties. The company reported that this manager violated Microsoft's policy and shared his/her account login information with 13 support representatives. As a result, third parties were able to partly reach Microsoft users' email accounts between 1 January 2019 and 28 March 2019.

- the Board announced that Microsoft notified the Board on 29 January 2020 due to a data misconfiguration on its security systems that lead to a breach which resulted in illegal disclosure of Microsoft customer records;

Maximum amount of penalty for a data breach



GEORGIA

Georgia adopted the Law of Georgia on Personal Data Protection of 28 December 2011 No. 5669 (Data Protection Act) on 28 December 2011, which serves as the fundamental legal framework for the country's data processing activities.

The Data Protection Act reflects Georgia's commitment to the 2005 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Additionally, the Data Protection Act was impacted by the Data Protection Directive (GDPR).

1. GOVERNING TEXTS

The Data Protection Act is further aided by other normative acts, including:

- Law of Georgia on State Inspector Service (N3273-RS, 21.07.2018)
- Resolution of the Government of Georgia on the Approval of the Regulations on the Activities of the Personal Data Protection Inspector and the Rule of Exercising the Power
- Order of the Personal Data Protection Inspector on the Approval of the List of the Countries Having the Appropriate Guarantees
- Order of the Personal Data Protection Inspector on the Approval of the Regulations of the Service.

In May 2019, the State Inspector Service (PDP) registered the Personal Data Protection Draft Law (Draft Law) as a bill in the Georgian Parliament. The Draft Law has yet to be subjected to three parliamentary hearings before becoming law.

The Draft Law's objective is to incorporate comprehensive data protection regulations into Georgian law and to ensure compliance with the General Data Protection Regulation (GDPR).

The PDP released a variety of guidelines and guides about the protection of personal data, including the following:

- Recommendations on Processing of Personal Data by the Commercial Banks
- GDPR – What You Should Know About EU Data Protection Regulation
- Recommendations on Processing of Personal Data in Health-

care
- The Guide for a Start-up
- Recommendations for the Internet Service Providers
- Recommendations on the Processing of Biometric Data
- Recommendations on the Video-surveillance
- Recommendations on the Personal Data Processing for Direct Marketing Purposes
- Recommendations on Processing of Personal Data by Financial Organizations
- Recommendations On Processing of Personal Data During Election and
- Recommendations On Processing of Personal Data During the Fight Against Covid-19.

In a recent judgment dated June 7, 2019, the Constitutional Court of Georgia reviewed the legal basis for sensitive data processing by Georgia's common courts.

The Constitutional Court overturned the normative content of Article 6 of the Data Protection Act, which prohibited the common courts of Georgia from disclosing court acts issued during open hearings in the form of public information.

2. SCOPE OF APPLICATION

The Data Protection Act applies to:

- processing of personal data through automatic or semi-automatic means on the territory of Georgia;
- processing of data through non-automatic means within the territory of Georgia, which data forms part of the filing system or are intended to form part of the filing system; and
- automatic processing of data defined as a state secret for the crime prevention and investigation, operational-investigative activities and protection of the rule of law.

Processing of personal data on Georgian territory will trigger the application of the Data Protection Act. If this is the case, the data controller's nationality or residence is irrelevant. The territoriality of the data processing activity is the deciding factor.

If the territorial criterion is not met, the Data Protection Act will apply to data

processing carried out by Georgia's diplomatic representations and consular offices abroad; and if the data controller is not registered in Georgia, data processing will be carried out using technical means available in Georgia. If this is the case, the data controller must appoint/designate a Georgia-based registered representative. If, on the other hand, such technical means are employed merely for the purpose of data transfer, the Data Protection Act is not applicable.

The Data Protection Act also has a material scope defined as follows:

- the processing of personal data through automatic or semi-automatic means;
- the processing of data via non-automatic means within the territory of Georgia which data forms the part of a filing system or is intended to form the part of the filing system; and
- the automatic processing of data defined as a state secret for crime prevention and investigation, operational-investigative activities, and protection of the rule of law except as provided by the Data Protection Act.

The Data Protection Act does not apply in the following circumstances:

- to data processing by a natural person for personal purposes not related to his/her entrepreneurial or professional activities;
- during court proceedings as far as it may prejudice the proceedings before the court's final decision is taken;
- to processing of data defined as a state secret for the purposes of state security (including economic security), defense, intelligence, and counterintelligence activities; and
- to the processing of information defined as a state secret, with certain exceptions.

Except as stipulated in Article 17 of the Data Protection Act, the Data Protection Act does not apply to the processing of data by media for public information or to the processing of information in the realms of art and literature.

The requirements that data controllers maintain a file system catalog and notify and register certain information with the State Inspector do not apply to political parties, professional and other unions, and religious groups processing data about their members.

The special category data processing rules do not apply to data processing for public safety, operational and investigative activities, and criminal inves-

tigations, unless the matter is expressly regulated in the Georgian Criminal Procedure Code, the Georgian Law on Operational-Investigative Activities, or other special laws, or unless the matter is specifically regulated in the Georgian Law on Official Statistics.

3. DATA PROTECTION & REGULATORY AUTHORITY

The Office of the State Inspector is the data protection regulator, having succeeded the Office of the Personal Data Protection Inspector. The State Inspector has three primary responsibilities:

- controlling the legality of data processing activities;
- monitoring of secret investigative actions and activities carried out in the central bank of electronic communication identification data; and
- investigation of crimes committed by the representatives of the law enforcement body, officers or persons equal to them.

The State Inspector, in addition to the powers mentioned above, may also carry out inspections of data processing activities in public and private organizations.

Additionally, the State Inspector may give data protection consulting to public and private entities, examine data subject applications, and maintain a registry of filing system catalogs.

4. KEY DEFINITIONS

Data controller: A public authority or natural or legal person which individually, or in cooperation with others determines the purposes and means of personal data processing and processes the personal data directly or via a data processor.

Data processor: Any natural or legal person processing the personal data for or on behalf of the data controller.

Personal data: Any information connected to an identified or identifiable natural person. A person is identifiable when he/she may be identified directly or indirectly, in particular by an identification number or by any physical, physiological, psychological, economic, cultural, or social features specific to this person.

Special category data: Data connected to a persons racial or ethnic origin, political views, religious or philosophical beliefs, membership of professional organisations, state of health, sexual life, criminal history, administrative de-

tention, putting a person under restraint, plea bargains, abatement, recognition as a victim of crime or as a person affected, also biometric and genetic data that allow to identify a natural person by the above features.

Health data: There is no definition of Health Data under the Data Protection Act.

Biometric data: Any physical, mental, or behavioral feature which is unique and constant for each natural person and which can be used to identify this person (fingerprints, footprints, iris, retina (retinal image), facial features).

Pseudonymisation: Data depersonalisation is defined as data modification in a way to make it impossible to link the data to the data subject or to require disproportionately great effort, expense and time to establish such a link.

Genetic data: Unique and constant data of a data subject relating to genetic inheritance and/or DNA code that makes it possible to identify them.

5. PRINCIPLES

Data controllers may process personal data in the form and manner permitted by the Law, including:

- to process personal and special category data;
- to process the data for direct marketing purposes; and
- to conduct the video-surveillance.

The main responsibility of the data controller is to ensure that the following requirements are met:

- there is a proper legal ground (such as, for example, data subjects consent) to process the personal data;
- the personal data is being processed for specific, clearly defined, and legitimate purposes;
- the personal data is processed only to the extent necessary for legitimate purposes;
- the personal data is adequate and proportionate to the purposes for which it was collected;
- the data is kept only for the period necessary to achieve the purpose of data processing;
- the data controller and data processor took necessary technical and organizational security measures to ensure the protection of personal data from accidental or illegal destruction, modification, disclosure, access, and any other form of illegal

use or accidental or illegal loss; and
- the security measures implemented by the data controller and data processor are adequate for the risks of personal data processing.

6. CONTROLLER AND PROCESSOR OBLIGATIONS

The necessity for registration (notice) also applies to databases. A database, as defined in Article 2(N) of the Data Protection Act, is any structured collection of personal data that is organized and searchable according to specific criteria. The phrase filing system is used in the Data Protection Act to refer to a database. For instance, a customer database or a registration of employees and clients that are processed may qualify as a filing system.

According to Article 19 of the Data Protection Act, the data controller is required to maintain a separate catalog for each filing system that contains a full description of the filing systems structure and content. Prior to the establishment of a filing system and the electronic input of a new category of data, the data controller must register with the State Inspector the following information:

- the name of the filing system;
- names and addresses of a data controller and a data processor, place of storing, and/or processing of data;
- legal grounds for data processing;
- the category of data subject;
- the category of data in the filing system;
- the purposes of data processing;
- the period for data storage;
- the fact and grounds for the restriction of a right of a data subject;
- the recipient of data stored in a filing system, and their categories;
- the information on the trans-border flows of data and transmission of data to an international organization, and the legal grounds for the transfer; and
- the general description of the procedure established to ensure data security.

Data controllers are responsible for maintaining an up-to-date file system catalog. Any modification to the information contained in the file system

catalog must be reported to the State Inspector within 30 days of the modification.

Notification is also required for cross-border data transfers and private companies' handling of biometric data.

Before using biometric data, a data controller must provide the Inspector with the same information as is supplied to the data subject, specifically the purpose of data processing and the security measures in place to secure the data subject's personal information.

Transfer of personal data outside Georgia is admissible without a separate authorisation from the State Inspector if one of the two following conditions apply:

According to Article 19 of the Data Protection Act, the data controller is required to maintain a separate catalog for each filing system that contains a full description of the filing systems structure and content. Prior to the establishment of a filing system and the electronic input of a new category of data, the data controller must register with the State Inspector the following information:

- a respective legal ground for data processing exists and the proper standards for the safety of data are secured in the relevant country; or
- the processing of data is stipulated in the international agreement between Georgia and the relevant country.

If neither of the above conditions applies, a formal written agreement should be entered into between the transferor and the receiver, in which the recipient commits to providing adequate safeguards to preserve the data. In this situation, the State Inspector must be supplied with the agreement and any other pertinent information or documents in order to obtain clearance for the data transfer.

The data processor is required to maintain records of all data processing actions performed on personal data that is stored electronically. Additionally, any disclosure or alteration of non-electronic personal data must be documented.

Currently, the Data Protection Act makes no provision for an obligation to do a Data Protection Impact Assessment/Privacy Impact Assessment. Appointing a data protection officer is not a mandatory necessity. There is no direct obligation to notify a data breach to the State Inspector.

The Data Protection Act makes no provision for the duration of data storage. The data controller chooses the duration of data retention on his or her own.

According to the general principle of the Data Protection Act, the personal

data may only be retained as long as necessary to achieve the legitimate objectives for which they were collected. After such purposes have been achieved, personal data must be blocked, deleted or destroyed, or retained in a form that prevents the identification of an individual, unless otherwise provided for by the Data Protection Act.

As confirmed by State Inspector rulings, it is not legal to store data indefinitely.

Article 71 of the Child's Code of Rights prohibits the disclosure of personal data about a child involved in administrative or judicial proceedings in any form, including through media, that could reveal or indirectly indicate the child's identity (an image, a detailed description of the child or his/her family members, names, addresses, audio and video recordings, and similar information).

Additionally, it is prohibited to disclose in any form, including through the media, a document or record containing personal data about a child that is related to the use of disciplinary measures against the child, violence committed against or by the child, the child's health status, the child's participation in social assistance or charity programs for disabled children or poor families, or other similar information.

The processing of special category data is prohibited except with the written consent of the data subject or where one of the following conditions apply:

- the data subject has made public the data about him/her, without expressly prohibiting the use of such data;
- processing of health related or prior conviction data is necessary for the data controller to observe the employment obligation, including for hiring the candidate;
- data processing is necessary to protect vital interests of the data subject or a third party and the data subject is physically or legally disabled to provide consent for data processing;
- the data are processed for the purpose of protecting the public health, processed by a healthcare facility (employee of such facility) for the purpose of protecting individuals health, or processed where necessary for the management or operation of the healthcare system;
- data processing is carried by political, philosophical, religious, or trade unity, association, or other non-commercial organization during performing the legitimate activities. If this is the case, data processing may only be related to the members of such organization or to the persons who have permanent connection with the organization;

- data is processed to run the registry/personal files of the accused/convicted individuals; to consider the issues related to individual planning of serving the sentence by the convicted person and/or releasing convicted person on a parole and changing of an unserved term with a lighter punishment; and
- data are processed in accordance with Law of Georgia On Crime Prevention, Non-Custodial Sentences, and Probation (only available in Georgian here), Law of Georgia On International Protection (only available in Georgian here), or for functionality of a uniform analytical system of migration data.

When processing special category data based on any of the grounds above, it is prohibited to publish or disclose to third parties the data without the consent of the data subject.

Data processing may be carried out by a data processor based on a legal act or written agreement concluded with the data controller. The agreement must meet the requirements of the Data Protection Act and other legal acts and include the prohibitions set out under the Data Protection Act.

8. DATA SUBJECT RIGHTS

Right to be informed: When personal data is collected directly from a data subject, the data controller or data processor must provide the data subject with the following information:

- identities and registered addresses of the data controller and the data processor (if applicable);
- purposes of the data processing;
- whether the provision of data is mandatory or voluntary and, if mandatory, the legal consequences of refusal to submit them; and
- the right of the data subject to obtain information on their personal data processed, request their correction, updating, addition, blocking, deletion, and destruction.
- Provision of the information is not mandatory if the data subject already has it.

Right to access: The data subject has the right to request information from a data controller on processing of their data. Upon request, the data controller must provide the data subject with the following information:

- which personal data was processed;

- the purpose of data processing;
- the legal grounds for data processing;
- the ways in which the data were collected; and
- to whom the personal data were disclosed, and the grounds and purpose of the disclosure.

The data subject must be provided with the above information immediately upon request or not later than 10 days after the request is made, when responding to the request it is required to:

- retrieve and process the information at another institution or structural unit or consult with either one;
- retrieve and process voluminous documents not linked to each other; and
- consult with its structural unit located in another populated place, or with another public agency.

Right to rectification: Upon the data subject's request, the data controller must correct, update, add, block, delete, or destroy the personal data if it is incomplete, inaccurate, outdated or collected in violation of the Data Protection Act.

Right to erasure: Upon request of the data subject, the data controller must delete or destroy the personal data if they are incomplete, inaccurate, outdated, or collected in violation of the Data Protection Act.

Right to object/opt-out: A data subject may revoke consent on data processing and request termination of data processing or deletion of processed data at any time and without explanation. This right of the data subject does not apply to the data processed with the consent and related to the performance of a monetary obligation.

Right not to be subject to automated decision-making: The Data Protection Act does not provide any specific provision on data subjects' right not to be subject to automated decision-making.

Right to appeal: The data subject may appeal the violation of their rights before the State Inspector, the Court, or the administrative body.

9. PENALTIES

A breach of the Data Protection Act can result in criminal, administrative, and civil liability.

Criminal liability: The unauthorized collection, retention, use, or dissemination of personal data that results in severe damage is punishable by a fine,

correction labor, and/or three years in prison. The legal entity may be fined, denied the right to conduct business, or forced into liquidation and fined.

Administrative sanctions: The State Inspector has the authority to order the suspension or termination of data processing, the blockage, destruction, or depersonalisation of personal data, the cessation of transfer, and the imposition of administrative fines.

The administrative fines provided under the Data Protection Act range from GEL 500 (approx. €125) to GEL 10,000 (approx. €2,500) depending on the type of violation.

Civil claim: Individuals may, in addition, bring a civil claim depending on the harm caused by the breach of the Data Protection Act.

Georgia's Supreme Court has rendered several important enforcement rulings. One of them concerns the processing of deceased individuals' personal data. The Supreme Court cited article 7.5 of the Data Protection Act, which allows for the disclosure of a deceased person's data for historical, statistical, and research purposes. The only exception is where the deceased person expressly banned dissemination of their data in writing, and the court determined that this is an acceptable legislative basis for processing the deceased's personal data. The Supreme Court stated, however, that the person seeking access to the deceased persons data on that basis must establish a statutory basis and compelling public interest for such access.

UNITED ARAB EMIRATES

The United Arab Emirates (UAE) has issued its first federal data protection law (Federal Decree Law No. 45/2021 on the Protection of Personal Data) (the Data Protection Law), alongside a law establishing the new UAE Data Office (Federal Decree Law No. 44/2021 on Establishing the UAE Data Office).

However, the executive regulations (Regulations) which will clarify various elements of the DP Law are yet to be released. The Regulations are expected to be issued within six months of the date of the issuance of the DP Law (i.e. before the end of March 2022). Businesses will then have a grace period of six months from the date of the Regulations to bring their organizations into compliance with the DP Law meaning enforcement is likely to commence from September 2022. Due to this, we will only cover what is currently in place on the federal scale in the UAE in this report.

In the meantime, the Constitution of the UAE gives citizens a general right to privacy, and provisions of the Federal Law No. 5 of 1985: The Civil Code as amended by Federal Law No. 1 of 1987 and the Federal Law No. 3 of 1987: The Penal Code (the Penal Code) are also relevant when considering privacy-related issues. Elsewhere, sector-specific regulation (such as telecommunications, consumer protection, and cybercrime laws) provides some limited data protection rights in certain circumstances.

The UAE plays host to a number of special economic zones known as free zones, which offer tax, customs, and other benefits to businesses. Of these free zones, the Dubai International Financial Center (DIFC), the Abu Dhabi Global Market (ADGM), and the Dubai Healthcare City (DHCC) have each enacted separate data protection laws applicable to businesses operating in the relevant zone.

- Government data and authorities
- The processing of health, banking, and credit data which is subject to sector-specific legislation
- Companies and institutions located in free zones which have specific data protection laws, such as the Dubai International Finance Center (DIFC) and the Abu Dhabi Global Market (ADGM)

Many organizations will therefore need to navigate both sectoral and free zone-specific data protection laws alongside the Data Protection Law.

The Data Protection Law will come into force on 2 January 2022. Some of the finer details will be set out in Executive Regulations, to be published by the Cabinet by the end of March 2022. Controllers and processors will have six months from the issuance of the Executive Regulations to comply with the Data Protection Law (around September 2022, depending on when the Executive Regulations are published).

The Data Protection Law does not set out any violations or penalties (these are expected to be issued by the Cabinet).

Article 31 of the Constitution is considered to represent the general right to privacy for citizens of the UAE, where it provides for the right to freedom and secrecy of communication by post, telegraph, or other means of communication under law.

The Civil Code and the Penal Code are also relevant. The Civil Code sets out certain obligations on employers when dealing with employee information, particularly on the termination of an employees employment (Article 913 of the Civil Code) and, separately, provisions on the basis for non-competition agreements where employees have access to their employers confidential information and/or client information (Article 909 of the Civil Code).

Article 378 of the Penal Code provides that it is a criminal offense to publish personal data which relates to an individual's private or family life. Furthermore, Article 380 of the Penal Code provides that anyone who opens correspondence without the consent of the intended recipient or overhears a telephone call also commits an offense. Article 380 also specifically prohibits the unlawful disclosure of correspondence and other information which comes to a person's knowledge in the course of his or her work.

Labor Law: Federal Law No. 8 of 1980 (Labor Law) regulates the maintenance of records relating to employees. Article 53 of the Labor Law requires every employer with five or more workers to:

- keep a special file for each worker showing his or her name, trade or occupation, age, nationality, place of residence, marital status, date of employment, remuneration, and any adjustments thereto,
- penalties imposed on them,
- occupational injuries and diseases he or she has sustained,
- and the date of and reasons for termination of his/her service; and
- create a leaving card for each worker to be kept in the workers file, divided into annual leave, sick leave, and other leave.

Article 54 of the Labor Law requires each employer with 15 or more workers to maintain in each place of business:

- a register of wages detailing the starting and leaving dates and salary of each employee;
- a register of work injuries;
- general workplace regulations; and

- a document detailing the penalties for employees in default. Infringement of the provisions of the Labor Law is punishable by imprisonment and /or a fine of not less than AED 10,000 (approx. €2,349).

Telecommunications Law: Article 72(6) of the Federal Law by Decree No. 3 of 2003 Regarding the Organization of the Telecommunication Sector (Telecommunications Law) provides that a person who intercepts the contents of telephone calls without prior permission by the competent judicial authorities may be punished with imprisonment for a period of not more than one year and/or a fine of not less than AED 50,000 (approx. €11,745) and not more than AED 200,000 (approx. €46,979). If a licensed operator reasonably believes that equipment is being used for the interception of telephone calls contrary to Article 72(6) of the Telecommunications Law, it may place the equipment under surveillance (Article 75 of the Telecommunications Law). Orders may also be issued for the seizure or destruction of the relevant equipment (Article 76 of the Telecommunications Law).

There are also requirements that derive from the Telecommunications Law with which only licensed operators are required to comply. Under powers granted to it by the Telecommunications Law, the TRA has issued the Consumer Protection Regulations (CPR). Article 12 of the CPR seeks to ensure the protection of data relating to subscribers, or persons who contract with licensed operators for the supply of telecommunications services in the UAE. "Subscriber information" is defined as any information relating to a specific subscriber, which includes a person's personal details, service usage details, the content of communications, account status, and payment history.

Licensed operators are subject to a number of obligations, including taking all reasonable and appropriate measures to protect the privacy of subscriber information (whether in paper or electronic form) and prevent its unauthorized disclosure or use (Articles 12.1 and 12.3 of the CPR). In addition, where it is necessary for a licensed operator to provide subscriber information to a third party that is directly involved in the supply of telecommunication services, the operator must require the third party to:

- take all reasonable and appropriate measures to protect the confidentiality and security of the subscriber information; and
- use the subscriber information only to the extent required to provide the relevant telecommunication service (Article 12.8 of the CPR).

Cybercrime Law: Article 2 of the Federal Law by Decree No. 5 of 2012 on Combating Cybercrimes (13 August 2012) (the Cybercrime Law) prohibits the unauthorized accessing of websites or electronic information systems or networks. This offense is punished by imprisonment (the period is not specified) and/or a fine not less than AED 100,000 (approx. €23,490) and not in excess of AED 300,000 (approx. €70,460). If an offense under Article

2 results in, among other things, the disclosure, alteration, copying, publication, and republication of data, it is punishable by imprisonment for a period of at least six months and/or a fine not less than AED 150,000 (approx. €35,234) and not in excess of AED 750,000 (approx. €176,169). If the data affected by an offense under Article 2 are personal, the offense is punishable by imprisonment for a period of at least one year and/or a fine not less than AED 250,000 (approx. €58,723) and not in excess of AED 1 million (approx. €234,892).

Article 15 of the Cybercrime Law provides that any person who intentionally and without permission captures or intercepts any communication through any computer network, website, or other information technology commits an offense. The offense is punishable by imprisonment (the period is not specified) and/or a fine not less than AED 150,000 (approx. €35,234) and not in excess of AED 500,000 (approx. €117,446). There is also a separate offense for any person who discloses information obtained unlawfully by receipt or interception of communications, which is punishable by imprisonment for a period of at least one year.

Article 21 of the Cybercrime Law establishes an offense relating to the invasion of privacy of an individual, by means of a computer network and/or electronic information system and/or information technology, without the individual's consent and unless otherwise authorized by law. This offense covers activities including eavesdropping and photographing and is punishable by imprisonment of a period of at least six months and/or a fine not less than AED 150,000 (approx. €35,234) and not in excess of AED 500,000 (approx. €117,446).

Article 21 also provides that a person commits an offense if he/she uses a computer network and/or electronic information system and/or information technology to amend a record or photograph for the purposes of defamation, to cause offense to another person or to invade another person's privacy. This offense is punishable by imprisonment for a period of at least one year and/or a fine not less than AED 250,000 (approx. €58,723) and not in excess of AED 500,000 (approx. €117,446).

Commercial Transactions Law: Articles 26 to 38 of the Federal Law No. 18 of 1993: Commercial Transactions Law (the Commercial Transactions Law) set out detailed provisions relating to the maintenance of commercial books. For instance, Article 30 for the same law, requires the trader to keep exact copies of the originals of all correspondence telegrams and invoices sent or issued by him or her for the purpose of his/her business activities, as well as all incoming correspondence (originals), telegrams, invoices, and other documents related to his/her trade, for a minimum period of five years from the date of issue or receipt.

Health Data Law: In the UAE, UAE Federal Law No. 2 of 2019 was enacted in May 2019, introducing noteworthy obligations around the collection, processing, and transfer of health data (as defined below) by a broad range of entities, including healthcare providers, medical insurance providers, healthcare IT providers, and providers of direct and/or indirect services to the

healthcare sector (for example outsourced services, including cloud services) located onshore, in the Dubai Healthcare City (DHCC), and in the Free Zones (Health Service Providers).

Health data is defined broadly to include all electronic data originating in the UAE regardless of its form, including alpha-numerical identifiers, common procedural technology codes, diagnosis and treatment, images produced by medical imaging technology, information collected during the consultation, lab results, and names of patients.

The Health Data Law seeks to protect health data in line with international best practice, as well as enabling the UAEs Ministry of Health both greater control over the sensitive data of its residents (as opposed to potentially putting it at risk in other jurisdictions) and a greater ability to collect and analyze health data in order to improve public health initiatives.

In May 2021, the UAE Federal Government issued Ministerial Decision No. 51/2021 on the Case of Allowing the Storage and Transfer of Medical Data and Information Out of the State (the Decision) to clarify concepts of the Health Data Law relating to restrictions on the collection, processing, and transfer of health data by a broad range of entities across the UAE. The Decision introduces exceptions to the general restriction on extraterritorial data transfers with related conditions and obligations attached. The Decision, therefore, provides further clarity to businesses in relation to the storage and transfer of health data and signifies a further step taken by the UAE to regulate personal data in accordance with the best international standards.

SUMMARY

Each of these countries targeted in this overview serves to explain a different policy issue that is important to address. We can summarize the overarching theme in two main headlines: beginner and advanced.

Countries that are closer to the European Union is much more advanced than the countries in the periphery of the European Union. the difference becomes more and more visible as we move towards the Middle Eastern peninsula. Cyprus is within the European Union borders meanwhile Turkey, and Georgia are immediate neighbors to the European Union. Turkey and Georgia have integrated online systems for their citizen that fosters the e-government policies. They also have advanced legislative systems that allow their citizen to protect themselves from data controlling and mining companies–locally and internationally.

Another great consequence of their cybersecurity legislation is that the data leaks and cyber-attacks during the Covid-19 pandemic has been very limited in these countries. As you can see in the report, it is not the case for other countries such as Lebanon, UAE, and Israel. We now know that governments should set up an agenda and take data protection and cyber-security serious immediately to not only protect their citizens from big companies but also to protect them from the government.

Israel is one of the more advanced countries when it comes to dat protection. They have a national data protection agency and have the necessary rules and regulations in place. We also know that they enforce these regulations through recent news about a major data leak from a credit card company, and some political party involvement with the national data.

Cyprus fully complies with GDPR as it is part of the European Union. Many private companies are registered in Cyprus due to the tax advantage reason and it is very important that Cyprus holds up the principles of data protection. Cyprus reported only four fines within the first year of the implementation of GDPR.

Lebanon is one of the most complicated countries when it comes to data protection. They were ahead in the game when they proposed a data protection law in 2018. However, they are still relying on international human rights charters for the basis of their data protection claims in 2021. Another problematic issue is that they do not have an independent data protection agency. Therefore, data within the country is handled between ministries of economy and trade, and defense. Doubtlessly, this does not fulfill the neutrality clause and creates tensions between stakeholders.

Turkey has the most structured system of data protection among all of these countries on this overview. They have enacted and implemented the data protection law since 2016. The board of data protection fulfills independency and neutrality clauses. They have strong indicators for a successful data protection outlook. There are only two major points to be improved: first, the Turkish data protection law is based on the predecessor of GDPR, which

is devised in 1995 to govern data protection in the European bloc. Second, the cap for fines are very low considering the weight of some of the very big companies in the country, it does not create the disincentivization factor.

On the other hand, Georgia has the most well-oiled system among all of these countries. Their data protection law is mostly aligned with the older version of European Union's GDPR; but they also implemented and integrated online systems into their governance very well. So much so that Georgia now considers itself an "e-democracy". With regards to the improvements, Georgia has the same problems as Turkey: low fines and outdated regulations compared to the GDPR–both can be addressed quite easily by smart policymaking.

United Arab Emirates is a new player in the game because up until January 2022, they did not have a separate data protection law; but rather scattered pieces of laws and regulations that are devised on case-basis. Up until 2022, they have been relying on their cybersecurity and telecommunications laws and the constitution to protect their citizens' rights.

Policy Recommendations – For Organizations and Individuals

Our first set of recommendation for all strategic partners of the European Union is to keep these six rules as their core principles:

- personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals;
- personal data shall be obtained for one or more specified, explicit and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- personal data shall be accurate and, where necessary, kept up to date;
- personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Following these, there are some key takeaways from the overview that we recommend policymakers to take into consideration.

Establish procedures. The data protection law should apply to all organizations, not only computer businesses or credit-rating agencies, but also other specialized industries. In this digital age, data protection is not only an aspect of corporate social responsibility; it is also an institutional risk and an essential compliance function for any organization that gathers, uses, or shares personally identifiable information or other potentially sensitive data of consumers.

Carry out Data Protection Impact Assessments (DPIA). A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and to minimize these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR. Under the GDPR, a DPIA is mandatory where data processing "is likely to result in a high risk to the rights and freedoms of natural persons"; however, DPIAs are a great tool to assess risks before going in to a new project no matter which data protection plan you are adhering to in your organization.

Protect by design and by default. You should guarantee that data protection risks are taken into account throughout the process of building a new product, policy, or service; rather than being treated as an afterthought, in accordance with the data protection by design philosophy. This entails conducting thorough assessments and putting in place appropriate technological and organizational safeguards and processes from the start to guarantee that the processing complies with the law and protects the data subjects' rights. To comply with the data protection by design and by default principles, you should guarantee that internal processes are in place to ensure that, by default, only personal data required for each specified purpose is handled.

Notify and report. Most organizations believe that a data breach is the end of their responsibility. That is not true: a well-established data protection policy also includes a crisis plan. Companies must report any losses or suspected breaches of personal data to a data protection agency as soon as possible. GDPR has the rule to report the breach within 72 hours of becoming aware of the breach; but it is a good practice to minimize the damage across the board for every organization. When the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, you are also required by law to notify the affected individuals without undue delay. Lastly, companies and organizations should build the necessary infrastructure for their consumers and employees to report if they discover or suspect a breach of data protection rule, loss or compromising of personal data.

Easy access to data protection tools and best practices. The easiest way to prevent data breaches and cybersecurity attacks is to equip every single individual with simple best practices and tools to protect themselves.

- Personal data should not be shared unless it is strictly neces-

sary with any public or private institution.

- Employees and individuals should keep their data secure by taking sensible precautions and following the guidelines provided by DPI or their company.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Strong passwords should be encouraged at all times and reliable virtual private network, 2FA authenticating, and password protecting applications should be encouraged and provided (free) for use.
- Individuals should be informed about the latest data protection technologies and should be given cybersecurity trainings in their line of work.
- parent manner in relation to individuals;
- personal data shall be obtained for one or more specified, explicit and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- personal data shall be accurate and, where necessary, kept up to date;
- personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Freedom of expression is a human right. Privacy is a human right. Human rights are essential to protect people from abuse, violence, and crime. For that, all laws affecting online speech or the use and sharing of personal data must adhere to human rights standards. Governments should refrain from implementing legislation that forces firms to violate, or facilitates the violation of, users' rights to freedom of expression and privacy. Government entities responsible for enforcing and enforcing laws must be subjected to rigorous and effective supervision. Individuals must be able to hold governments accountable for how they exercise power over online speech and personal data.

About the Author

Nazlican Kanmaz
Research Director

Nazlican Kanmaz is the research director at B&K Agency. Nazlican has worked for non-profit organizations in Turkey, Germany, the UK, and the Netherlands. She is experienced in political consulting and brand strategy for creative agencies and has been a certified Council of Europe trainer and facilitator for four years.

Nazlican speaks Turkish and English and holds a master's degree in Philosophy of the Social Sciences at the London School of Economics and Political Sciences.

Resources

- https://www.haaretz.com/israel-news/tech-news/.premium-how-not-to-use-whatsapp-israeli-credit-card-firm-learns-tough-lesson-1.10165329
- https://www.grcworldforums.com/data-protection-and-privacy/political-parties-violated-israels-privacy-protection-law/747.article
- https://www.kvkk.gov.tr/Icerik/6694/PUBLIC-ANNOUNCEMENT-DATA-BREACH-NOTIFICATION-Microsoft-Corporation
- https://smex.org/an-ugly-new-data-protection-law-in-lebanon/
- https://www.accessnow.org/cms/assets/uploads/2021/01/Access-Now-MENA-data-protection-report.pdf
- https://www.the961.com/lebanese-info-public-facebook-data-leak/
- https://www.bbc.com/news/technology-50207192
- https://www.dataprotectionreport.com/2016/06/uae-employees-jailed-for-privacy-breach-before-ultimately-being-acquitted/
- https://www.globalprivacyblog.com/legislative-regulatory-developments/uae-publishes-first-federal-data-protection-law/
- https://www.lexology.com/library/detail.aspx?g=bd78c069-b7bf-4f29-a973-d2e7f29c644c
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/925300/data-protection-policy.pdf
- https://rankingdigitalrights.org/governments-policy/
- https://www.cfr.org/report/reforming-us-approach-data-protection
- https://freedomhouse.org/policy-recommendations/internet-freedom

AGENCY

347 Fifth Ave, Suite 1402
New York, NY
10016

+1 (434) 264-1485
hello@bkagency.co
www.bkagency.co