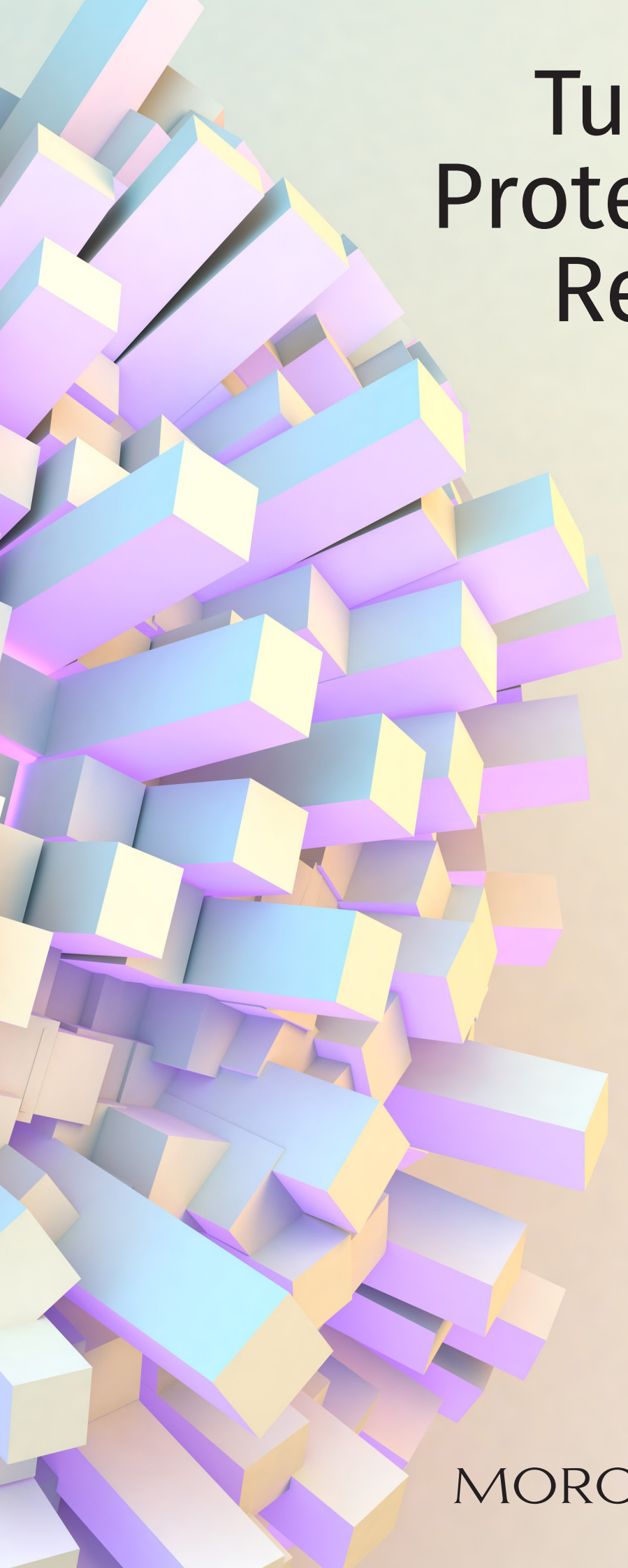


Turkish Data Protection Law Review 2021

First Five Years in Practice

MOROĞLU ARSEVEN

Foreword

In the five years since the enactment of Personal Data Protection Law No. 6698, much of what were once considered standard business practices have become obsolete, if not unlawful.

Data controllers are now required to implement within their operating frameworks specific safeguards to protect personal data. For some data controllers, compliance necessitated a rethinking and redesigning of their business, as it were, from the ground up.

September 2020, marked the end of the registration period for data controllers to register as private entities whose main business activity does not involve processing special categories of personal data. During the registration process, many data controllers were investigated by the Personal Data Protection Board, and some were fined or otherwise sanctioned for non-compliance.

Notably, for many data controllers cross-border transfer of personal data in compliance with current regulations remains a challenge. The legal and business communities await both publication by the Personal Data Protection Board of a comprehensive list of safe countries, and amendments to enacted legislation which are expected to address Turkey's goal of closer alignment with the General Data Protection Regulation.

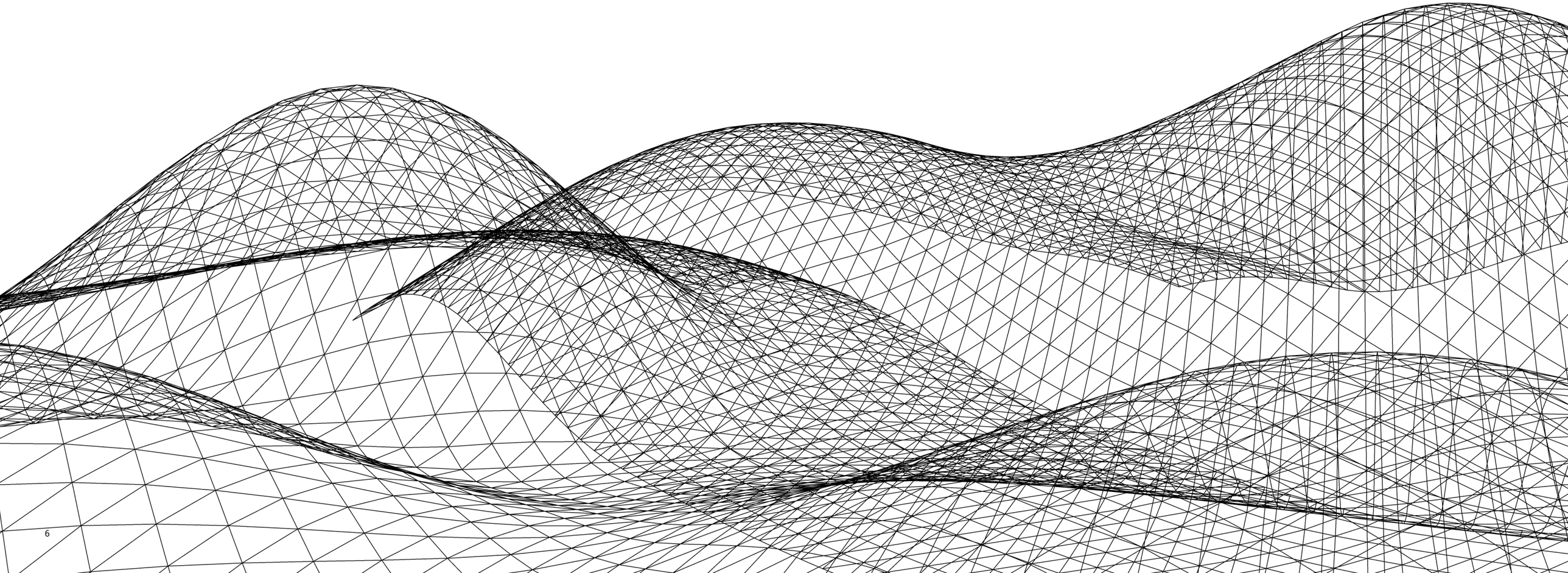
In recognition of Data Privacy Day, Moroğlu Arseven presents this five-year retrospective survey of developments in Turkish data protection law. Given the evolving nature of the statutory landscape, we will update this survey when necessary, and encourage you to stay current by returning to it periodically.

Contents

MOROĞLU ARSEVEN

MOROĞLU ARSEVEN

I. BACKGROUND



A. Enforcement Processes

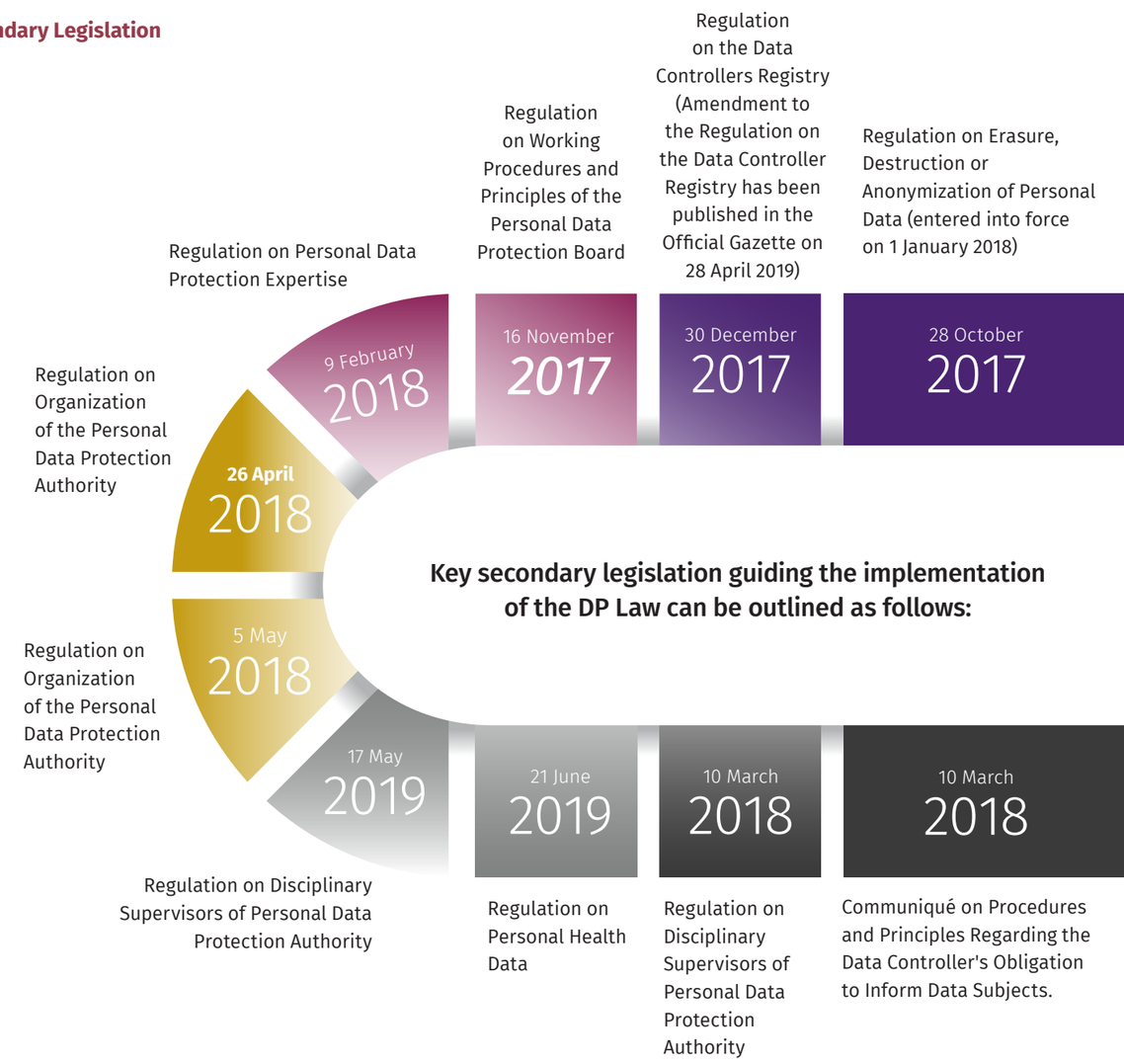
1. Enactment Process of The DP Law

Personal Data Protection Law No. 6698 ("**DP Law**") came into force in Turkey on 7 April 2016 after long-lasting efforts and debates on several other draft bills. In fact, a specific data protection law was first referred to in 2003, as part of the harmonization process for Turkey's accession to European Union ("**EU**") membership. As of that time, many draft bills on data protection had been submitted to the Turkish Parliament, yet none were enacted.

Until the enactment of the DP Law in 2016, the protection of personal data was regulated unmethodically by several Turkish statutes (e.g., the Turkish Constitution, Turkish Criminal Code, Turkish Code of Obligations, and Turkish Labor Law, etc.), and certain sector-specific regulations. However, those laws were not adequate to ensure the necessary level of data protection in Turkey, which could be achieved by a comprehensive data protection law. In this context, on 24 March 2016, the DP Law was adopted, then published in the Official Gazette on 7 April on 2016.

As it is the first primary source regulating data protection in Turkey, the DP Law included certain transitional provisions to regulate the compliance period (Provisional Article 1 of the DP Law). Accordingly, market players were granted a two (2) year transition period within which to become fully compliant with the DP Law. That transition period concluded prior to publication of this article.

2. Secondary Legislation



In addition to the statutes and regulations mentioned above, regulatory and supervisory decisions, as well as guidelines, of the Turkish Data Protection Board ("**Board**") have shed light on the implementation of the DP Law. (Please see Section II.C) for further information on Board decisions).

B. Regulatory Structure

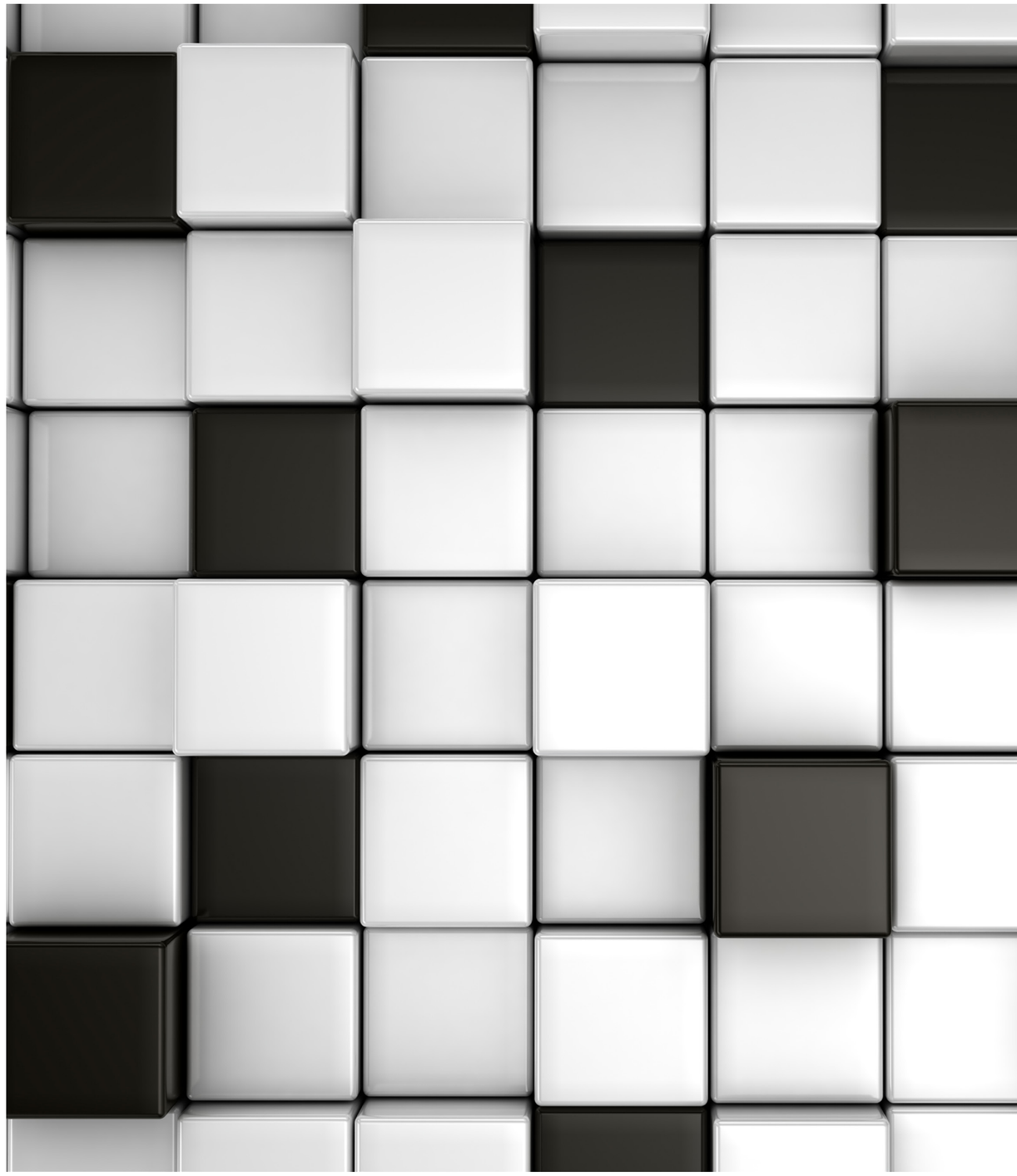
In order to ensure proper implementation of the data protection rules, the Personal Data Protection Authority ("**Authority**") was established as an independent regulatory authority, with organizational and financial autonomy, charged with ensuring fulfillment by market players of all provisions of the DP Law. The Authority is composed of the Board and the Presidency. The mission of the Authority is to provide protection of personal data and to develop public awareness of the fundamental rights related to privacy and freedom protected by the Turkish Constitution; and to establish an environment to enhance the competition capability of public and private organizations in the data driven world economy.

The Board is the Authority's decision making body, consisting of nine members, five of which are appointed by the Grand National Assembly of Turkey, and the remaining four by the President of the Republic. The Board has been active in Turkey since January, 2017.

The Board's duties can be summarized as follows:

- to ensure that personal data processes are in compliance with the DP Law,
- to promulgate rules and regulations under the DP Law,
- to determine and announce which countries abroad provide adequate data protection, and which do not, and to permit transfer of personal data abroad if the controllers both in Turkey and abroad guarantee in writing the existence of adequate data protection,
- (if considered necessary) to announce data breaches on its official website or through other methods it deems appropriate,
- to examine and conclude complaints related to data protection,
- to decide whether processing of data or transfer of data abroad shall be stopped to prevent damages, difficult or impossible to recover, and if it such processing or transfer is clearly unlawful,
- to maintain that the data controllers' registry system,
- to conduct disciplinary investigations against civil servants, and to decide on administrative sanctions,
- to carry out regulatory procedures,
- to approve and publish draft reports regarding its administrative functions.

The Board also established an Information Hotline (ALO 198) to provide information regarding the registration procedure of VERBİS and other necessary steps to be taken for data protection matters.



C. Fundamental Concepts

Personal Data includes any information relating to an identified or identifiable real person. Therefore, any information that can be used to identify an individual would constitute personal data. For example, a customer's name and address, IP address, e-mail address, or a database of customer email addresses.

Special Categories of Personal Data is a type of Personal Data which receives extra protection. These include information which reveals 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, punitive measures, and biometric and genetic data. Notably, protection regarding appearance, criminal records, punitive measures, biometric and genetic data go beyond the framework in the referred EU legislation regarding special categories of data.

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 a Data Controller.

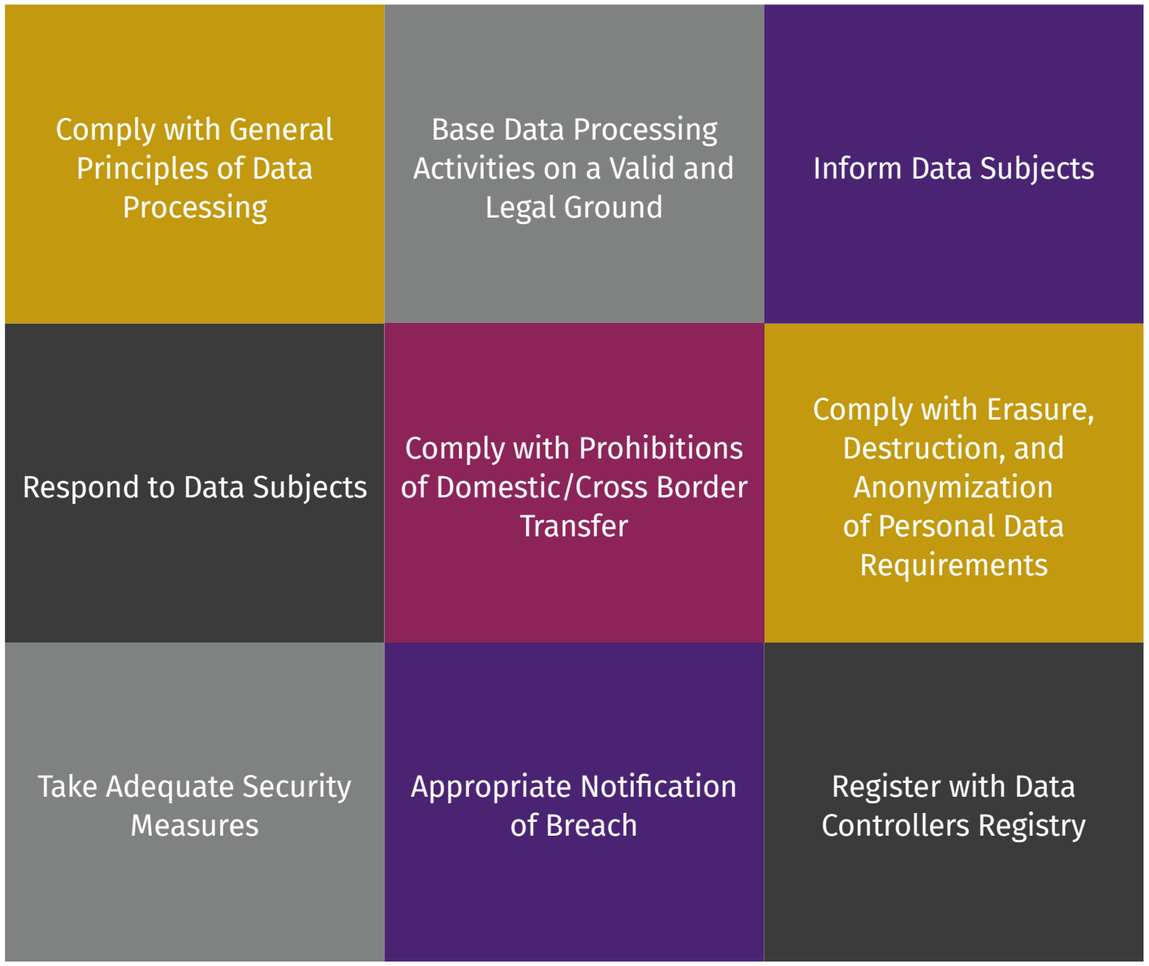
Explicit Consent means informed consent given freely and at the will of a data subject. The DP Law introduces a general prohibition on processing Personal Data or Special Categories of Personal Data without explicit consent. However, it does not envisage a specific method to obtain such explicit content. In light of that, 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.

VERBİS is the Data Controllers Registry System where data controllers register their personal data processing activities according to certain promulgated criteria.

MOROĞLU ARSEVEN

D. Obligations of Data Controllers and Data Processors Under the DP Law



1. Principles of Lawful Data Processing

The following key principles need to be followed in all personal data processing activities (Article 4 of the DP Law) performed by data controllers. Personal 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.
- Retained for the period determined by relevant legislation, or as deemed necessary for the purpose of the data processing.

Decisions on Principles and Conditions for Lawful Data Processing	
Decision Number	2019/331
Board Ruling	Data controller failed to take necessary technical and administrative measures to prevent processing of personal data without a legal basis
Decision Number	2019/81 - 2019/165
Board Ruling	Data controllers failed to take necessary technical and administrative measures to prevent processing of special categories of personal data without a legal basis and to ensure compliance with the principle of proportionality
Decision Number	2019/294
Board Ruling	Data controller failed to take necessary technical and administrative measures to prevent processing of personal data without a legal basis, to ensure that the principles under the DP Law are complied with and rights of data subjects are respected.
Decision Number	2019/ 188
Board Ruling	The Board decided that the announcement method conducted by the university allowed access to third parties without relying on any legal basis under the DP Law

2. Conditions of Lawful Data Processing

In addition to the main principles discussed above, current legislation envisages various legal grounds for processing personal data and special categories of personal data[1] to ensure an adequate protection under the DP Law.

Article 5 of the DP Law envisages the legal basis for data processing. Accordingly, personal data can be processed in the following cases:

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

Regarding special categories of personal data, narrow legal grounds have been introduced for processing. Accordingly, special categories of personal data may only be processed if the data subject explicitly consents. In terms of additional legal bases for processing, the DP Law divides special personal data into two categories:

- Personal data related to health or sexual life,
- Other special categories personal data.

While other types of special categories of personal data can be processed, if such processing is permitted by law, personal data related to health or sexual life is more strictly protected relative to other special categories of data, and, as such, legal grounds for processing are 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 by persons operating under 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,
- Planning and management of health care services and their financing.

[1] Data related 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.

MOROĞLU ARSEVEN

The Ministry of Health ("**Ministry**") published the Health Regulation ("**Health Regulation**") in the Official Gazette dated 21 June 2019 and numbered 30808, repealing the previous Regulation on Processing and Ensuring the Privacy of Personal Health Data, published in the Official Gazette dated 20 October 2016, and numbered 29863. The Health Regulation sets forth the personal health data processing regime with which public institutions and private entities must comply, and reveals a more detailed approach inasmuch as it regulates concealment, correction, and abolishment situations for health data in specifically tailored subsections.

The Health Regulation is binding on all private, natural, and legal persons, and public legal entities who process personal health data, and introduces comprehensive rules and procedures related to the rights of data subjects under the DP Law. Such comprehensiveness, particular regarding data access, is intended to increase protection for personal health data. However, it is within the Board's discretion to determine whether precautions under the Health Regulation are adequate to protect personal health data.

Moreover, the Health Regulation requires implementation of anonymization, masking measures, and identification restrictions to prevent revealing the data subject in case of unauthorized acquisition of personal health data.

The Health Regulation also introduces provisions regarding access to personal health data by healthcare institutions, and specifically limits access to personal health data by healthcare workers unless required for provision of healthcare services. In that regard, the Regulation provides that accounts on e-Pulse (e-Nabız) - the online healthcare portal established by the Ministry in accordance with e-government practices - can be accessed only in accordance with the specific privacy settings of those accounts as set by the associated data subject. Thus, by changing their privacy preferences data subjects can restrict access of healthcare institutions to health data stored on their e-Pulse accounts.

In addition, as part of the limitations provided by the Health Regulation, attorneys can no longer access client personal health data by relying on a general Power of Attorney. The Health Regulation requires data subjects to include in Powers of Attorney an explicit declaration of consent to the empowered attorney's access to personal health data.

The Health Regulation includes a provision governing access to the personal health data of a deceased. It provides that personal health data of a deceased will be stored for a minimum of twenty (20) years, and the legal heirs of a deceased shall be individually authorized to access such data.

Clearly, the Health Regulation is an instrument important for protecting personal health data, the processing of which involves multiple actors, and requires various levels of protection. The Ministry, following in the footsteps of the EU – specifically, its General Data Protection Regulation ("**GDPR**") - has not only enacted the new Regulation, but in an effort to ensure its longevity, drafted it with reference to EU guidelines.

The Board has delivered several decisions regarding health data, one of which gained considerable media coverage because the data subject was a famous person. In that Board decision, dated 31 January 2018, and numbered 2018/10, an individual's health report containing special category personal data was shared widely on the internet and social media by the data subject's physicians in relation to certain inpatient medical. In response, the Board imposed an administrative fine on the data controller who, it was determined, failed to provide security sufficient to protect personal data under both subparagraph (c) paragraph (1) of Article 12, and Article 18 of the DP Law.

2.1 Explicit Consent as Legal Basis

In accordance with certain secondary legislation, including, but not limited to, the guidelines and resolutions of the Board, a data controller may assert explicit consent as the basis for processing personal data only where other legal bases are not applicable. In fact, the Board considers obtaining explicit consent to be misleading and potentially violative of the rights of the data subject where other applicable bases are available under applicable law. Therefore, it is crucial for data controllers to determine all applicable legal bases for data processing before seeking the consent of data subjects.

As defined under Article 3 of the DP Law, explicit consent should be freely given, specific, and informed. As elaborated by the Board, explicit consent can only be given by a statement or by a clear, affirmative action constituting an unambiguous indication of a data subject's agreement to the processing of his/her personal data.

For an explicit consent to be unambiguous, the data subject's statement or clear, affirmative action must leave no doubt as to his/her intention to consent and be a deliberate and specific opting in or agreeing to data processing activity. Therefore, silent consents obtained by opt-out methods such as pre-ticked boxes are deemed invalid by the Board.

The DP Law and its secondary legislation allows explicit consent to be given on paper, or electronic form provided, however, that, unless otherwise provided under applicable law, the consent procedure includes electronic or digital signatures, icon clicks, checkboxes, or confirming emails. Unlike Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, the DP Law does not require explicit consent be in writing, and may be obtained through electronic means, call centers, etc. Regardless of the method employed to obtain explicit consent, the burden of proof rests with the data controller.

Explicit consent freely given requires that the data subject made a genuine, unequivocal choice, and must be able to refuse or withdraw the consent. The Communiqué on Procedures and Principles Regarding the Data Controller's Obligation to Inform ("**Disclosure Communiqué**"), and the guidelines of the Board require data controllers to provide a wholly separate document just dealing with obtaining consent. Moreover, the Board clearly indicated in its resolution numbered 2018/90, that explicit consent must be obtained through a document different to and separate from any general privacy notice, and must constitute a voluntary opting in. For online processing activities, the resolution also provides that approval of the privacy notice and explicit consent cannot be together obtained through one and the same check box.

Additionally, the above discussed resolution states that explicit consent should not be relied upon where there is a clear imbalance of power between the data subject and the data controller, for example, an employer-employee relationship where a consent may be coerced or obtained under duress.

Explicit consent must be informed such that a data subject is provided with a privacy notice that has all necessary details of the processing activity in a language and form they can understand. This should allow data subjects to comprehend how the processing will affect them. The responsibility lies with the data controller to demonstrate that the data subject has been informed and explicitly consented to the processing.
As stated in the Board's guidelines, explicit consent must also be specific, meaning it must be given specifically for that processing activity. Therefore, a data controller should clearly explain the specific reason for and proposed use of the data so that based thereupon a data subject can with specificity explicitly consent.

Furthermore, giving explicit consent is a right strictly attached to the data subject who has the right to determine the future of his/her personal data. Therefore, a data subject can withdraw his/her explicit consent at any time. Withdrawal of explicit consent applies to all data for which the original, explicit consent was obtained, and all processing of such data must cease upon the withdrawal.

It is worth noting that for data controllers, it is vital to choose legal grounds appropriate to their processing activity. Data controllers should avoid seeking explicit consent in any processing activity where other legal grounds are applicable under the circumstances. Data controllers must not forget that explicit consent should be freely given, specific, and informed. Therefore, before commencing any processing activity, they need to confirm that the consent obtained is appropriate under the circumstances and valid under applicable law before. In a decision dated 2 August 2018, the Board reiterates that if grounds exist for processing personal data other than explicit consent, then obtaining such consent from a data subject is an abusive, misleading, and invalid under applicable law.

2.2 Exceptions to Explicit Consent

Under specific circumstances deemed exceptional cases, the Board grants an exemption from the explicit consent requirement of the DP Law.

a) Permitted by laws: If explicitly provided for by law, personal data may be processed without data subject's explicit consent; provided, however, that a specific, unambiguous recitation of the grounds for processing such personal data must be made. 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 are examples of processing activities permitted by law.

b) Protection of life or physical integrity: Personal data can be processed in protection of life or physical integrity of a person, or of any other person who is bodily incapable of giving his/her 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.

c) Conclusion or fulfilment of a contract: Personal data of each party to a contract may be processed by the other party provided that it is strictly necessary to close or perform the contract, for example, processing personal information of an employee by an employer in order to finalize an employment agreement.

d) Performance of legal duties: If processing data is legally compulsory for a data controller to fulfil its legal duties, it is allowable to the extent that it is necessary for and relevant to fulfilling the legal duty. In this respect, an employee's financial data can be processed by the employer for the wage payment, a recipient's address data can be processed by a cargo carrier.

e) Publicly available data: Personal data that has been made public by the data subject can be processed but only in accord with and limited to the purpose for which the data subject originally made the data public. For example, if a person discloses his phone number in order to receive inquiries about a vehicle he is selling, the phone number may be processed only to facilitate such inquiries.

f) Establishment, exercise, or protection of any right: Personal data may be processed if it is crucial to establishing, exercising, or protecting a right. For example, where a lawsuit is filed against an employer, certain personal data of the employee can be processed and transferred to the court to defend the employer's rights.

g) Legitimate interest: As per the DP Law, 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. For example, the preamble of the DP Law provides 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 constitute legitimate interests of the company. The legislation also indicates that although the explicit consent of a data subject is not required in these cases, fundamental principles of personal data protection should still be complied with, and the interests of the data controller and those of the data subject should be weighed.

According to the GDPR, processing personal data on the basis of a legitimate interest should be lawful and not override fundamental rights of the data subject based on the following three criteria: (i) necessity, (ii) existence of legitimate interest, and (iii) balancing exercise. Therefore, after conducting a balancing test between the interests of the data controller and the rights and freedoms of the data subject, if it is possible to say that processing personal is a necessity, then it may be accepted as a legitimate interest of the data controller. Although the DP Law provides that the personal data may be processed without obtaining consent if there is a legitimate interest of the data controller, neither the DP Law nor the Board provides a balance test or any certain criteria for evaluating the interests of the data controller or the fundamental rights and freedoms of the data subject.

Since both (i) using legitimate interest as a ground for lawful processing is far more complicated than merely having a legitimate interest to process personal data, and (ii) the approach of the Board is not yet certain, if there is another exception that the data controller can rely on, it should do so.

3. Obligation to Inform

To ensure transparency, it is mandatory under Article 10 of the DP Law, that a data processor, regardless of the legal basis for data processing, must, when collecting personal data, inform the data subject as follows:

- Identity of the data controller and its representative, if any,
- Purpose of personal data processing,
- Recipients to whom the personal data can be transferred, and the purpose of the transfer,
- Methods of and legal reasons for collecting personal data,
- Rights of the data subject under the DP Law.

The obligation to inform is not subject to a request from the data subject, and must be fulfilled not later than the time of obtaining the personal data.

The methods to be used for providing privacy notifications are specified in the Disclosure Communiqué; pursuant to which, notifications may be provided either physically or by using electronic means, including verbally, in writing, by voice recording, or through call centers. Yet, the burden of proof will remain on the data controller to show that it has complied with all notification obligations under the DP Law. The Disclosure Communiqué also states that notification must be provided separately from any explicit consent, or any other agreements, including, but not limited to, general privacy agreements or terms of use. Thus, and pursuant to Board decision, numbered 2018/90, and dated 26 July 2018, a data controller must fulfill separately its information obligations and its obtaining, where necessary, explicit consent of a data subject.

Decisions regarding Obligation to Inform and Explicit Consent as Legal Basis	
Decision Number	2018/90
Board Ruling	Confirmation of privacy notice and obtaining explicit consent processes need to be conducted separately.
Decision Number	2019/82
Board Ruling	Obtaining explicit consent for loyalty card practices do not violate the principles of the DP Law. The chain's privacy notice and anonymization practices are not compliant with the DP Law.
Decision Number	2019/206
Board Ruling	Explicit consent can only be used as a legal basis by a data controller where other legal bases are not applicable. Confirmation of privacy notice and obtaining explicit consent need to be conducted separately.

4. Transfer of Personal Data

4.1 Conditions of Data Transfer

The same legal grounds for processing or transferring personal data within Turkey apply when the processing or transfer is international (see, Article 8 of the DP Law). In this regard, statute requires that processing or transferring personal data within Turkey, by, to, or between data controllers or processors, must be supported by at least one legal ground provided by Article 5 of the DP Law.

It is worth noting that, unlike the GDPR, the DP Law envisages no specific rule applicable to data transfers from data controllers to data processors, hence transfers to third parties and transfers to data processors/controllers are equally subject to the DP Law.

4.2 Conditions of Cross-Border Data Transfers

a. Current Cross-Border Data Transfer Regime Under the DP Law

As per Article 9 of the DP Law, cross-border data transfers shall be based upon one of the following legal grounds:

- the data subject has given his/her explicit consent, OR
- the cross-border transfer is based on grounds se forth in the DP Law, including:
  i. The receiving country must be determined by the Board to safe, and to provide with adequate data protection, or
  ii. If the level of data security is not adequate, then data transferor in Turkey and data receiver abroad (data controller or processor) must execute a written letter of undertaking (the minimum content of which has been determined by the Board), and thereupon seek approval of the Board to perform the data transfer.

The Board has not yet published a comprehensive list of countries providing adequate data protection. It is therefore prudent to consider all countries outside Turkey as conuntires without adequate level of protection for data transfers. At the present state of affairs, there are two statutory ways for a data controller to transfer personal data abroad; (i) obtaining explicit consent of the data subject, or (ii) approval of the Board upon a written undertaking executed by the data transferor and data receiver. The Board published on its website standard terms for data transfers, including the requirement that a written undertaking executed by the data transferor and the data transferee must, at a minimum, recite such standard terms; which are essential clauses that must be included in agreements for transferring personal data to countries without adequate level of protection; and which terms include separate provisions for transfers to data controllers and data processors. The minimum content required by the Board is quite similar to EU Standard Clauses.

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 both for multinationals and local companies with cross-border operations, or data servers maintained outside of Turkey. The Board can limit cross-border data transfers if determined to be against the public interest, or personal interests. It is not yet clear how the Board will make determinations of violation.

b. Binding Corporate Rules

Lack of a comprehensive list of countries with adequate level of protection by the Board causes operational and legal problems for multinational companies which in the ordinary course of business transfer personal data for organizational, infrastructural, and reporting purposes. In this context, and considering the needs of market participants and their often complex, grouped corporate structure, on April 10, 2020, the Board, announced Binding Corporate Rules ("**BCR**"), modelled after the European Union's BCR approach, which allow intra-group data transfers among multinationals.

BCR is defined as data protection rules applicable in cross-border transfer, and allow multinationals operating in countries without adequate level of protection to undertake adequate data protection for corporate intra-group data transfers.

The BCR introduced by the Board allows multinationals to transfer personal data from Turkey to a member of the same corporate group located in a country with inadequate data protection. In such cases, the BCR itself is be considered a commitment to provide adequate data protection for intra-group, cross-border data transfers.

BCR must include all general data protection principles and adequate safeguards for protecting personal data in the corporate group. The Board provides a guideline on required content of BCR, and a standard application form on its official websites. Required BCR elements and principles of BCR are as follows:

- Binding Nature
- Effectiveness
- Coordination with the Board
- Principles on Processing and Transfer of Personal Data
- Mechanism for Reporting and Recording Changes
- Data Protection Safeguards
- Accountability and Other Tools

In addition to the above, applicants can insert certain non-mandatory, auxiliary clauses in BCR to ease the application process.

Multinationals seeking to base intra-group, cross-border data transfers on BCR need to make necessary preparations including, drafting BCR in accordance with the Board's guidance, filling out the application form published by the Board, and applying to the Board, with all required documentation, for approval of BCR. Applications will be concluded by the Board within one (1) year of the official application date. If necessary, the Boad can extend this period for an additional six (6) months.

The Board announced, on 26 October 2020, revision requirements for lawful cross-border data transfers; which, in relevant part, provided that the Convention 108 alone does not provide adequate grounds for lawful cross-border transfer, notwithstanding prior Board decisions to the contrary.

In a previous Board decision, numbered 2020/173, and dated 27 February 2020, Amazon transferred user data to both the EU and USA, based upon a written undertaking submitted to the board, but without obtaining the explicit consents of the data subjects. According to the Board: "In the examination, it was seen that the data controller submitted letters of undertaking to the Board to obtain the approval of the Board in order to transfer data abroad. However, considering that the Board has not yet made a decision in this direction and countries with sufficient protection have not yet been determined, the only method for transferring personal data abroad is considered to be the explicit consent of the person concerned". In the decision, numbered 2020/559, and dated 22 July 2020, the Board again confirmed, as it had done in the Amazon decision, that, with respect to cross-border data transfers, Convention 108 is not an alternative to the DP Law.

Decisions regarding Data Subject Rights	
Decision Number	**2019/157**
Board Ruling	The Board ruled that use of email services that store data is a cross-border data transfer.
Decision Number	**2020/173**
Board Ruling	The Board ruled that since no explicit consent was obtained for cross-border data transfer, and since Amazon Turkey's undertaking had not been yet been approved by the Board, a cross-border data transfer by Amazon Turkey was unlawful.
Decision Number	**2020/559**
Board Ruling	The Board ruled that personal data cannot be transferred abroad solely based on Convention 108, and that the DP Law must be strictly followed.

5. Obligation to Respond to Data Subject Requests

Since 7 October 2016, data subjects have been entitled to request the following from data controllers (see, Article 11 of the DP Law):

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

5.1 Procedural Details

The Board has issued the Communiqué on Principles and Procedures for Application to Data Controller ("**Application Communiqué**"), which regulates the methods and procedures for lodging a request with a data controller. Accordingly, data controllers should respond to requests duly lodged by data subjects within thirty (30) days. The Application Communiqué also provides for a processing fee of one (1) Turkish Lira for each page for responses exceeding ten (10) pages, or a fee equivalent to the cost of the data recording medium (such as CDs and flash disks, if the response is given in this manner).

The Board has clarified the periods for filing complaints to the Board and applying to data controllers stipulated under the Articles 13 and 14 of DP Law. According to the Board decision, numbered 2019/9, and dated 24 January 2019, the following principles apply when calculating application periods:

- If the data controller fails to responds within 30 days, the data subject has 60 days to apply to the Board, starting from the date of its application to the data controller.
- If the data controller responds within 30 days, the data subject can file a complaint with the Board no later than 30 days after such response.
- If the data controller reponds after the 30 days period has lapsed, the data subject can file a complaint with the Board no later than 60 days following the date of application to the data controller; which complaint may be submitted immediately upon expiration of the 30 day period, whether or not a response has been received from the data controller.

Decisions regarding Data Subject Rights	
Decision Number	**2020/41**
Board Ruling	Data subject's compensation claims arising out of violation of personal rights must be raised before the general courts.
Decision Number	**2019/296**
Board Ruling	The Board ruled that the data controller's, which is an operator company, limited available application methods violates the Article 6 of the Communiqué on the Procedures and Principles of Application to the Data Controller.
Decisions regarding the Board's Competence	
Decision Number	**2018/156**
Board Ruling	Notices and complaints related to matters that fall within the mandate of judicial authorities cannot be reviewed by the Board.
Decision Number	**2019/138**
Board Ruling	Notices and complaints related to matters that fall within the mandate of judicial authorities cannot be reviewed by the Board.

5.2 Advisory Step Plan

- Data subject requests are forwarded to the relevant department within the data controller or data protection committee, if established.
- Significance of, level, and type of data subject request is determined. Data subject requests may be categorized as follows; (i) information requests regarding personal data processed within data controller, (ii) deletion requests regarding personal data processed within data controller, and (iii) information requests regarding specific personal data processing activity within data controller.
- In order to respond to the data subject's request within 30 days, as stipulated by the DP Law, data controllers should use a tracing system.
- In the case information requests or information requests regarding specific personal data processing activity, the appropriate department within the data controller will prepare an official response and deliver it to the data subject by means allowable under the DP Law. In the case of a deletion request, the appropriate department, and either in-house legal staff or outside counsel will decide whether or not to delete personal data based on its deletion and destruction policy. In the event of a decision to delete personal data, log records regarding that process should be kept, and a formal notification should be provided to the data subject.

6. Erasure, Destruction, and Anonymization of Personal Data

Personal data shall be maintained for the purpose for which they are processed, as required by the limitation of purpose. In this regard, a data controller is obliged to take following administrative and technical measures:

- establishing personal data retention and erasure policy and principles,
- determining storage periods as well as technical and administrative measures to be applied in connection with storage,
- ensuring storage of personal data in accordance with these principles.

Data controllers shall comply with the periods set forth in the legislation for relevant personal data. In the event that the length retention cannot be estimated, the data shall be retained only as long as necessary for the purpose for which it is being processed.

Data controllers are obliged to erase, destroy, or anonymize personal data (i) *ex officio*, (ii) upon the demand of the data subject, and (iii) if the reasons for which it is being processed are no longer valid (see, Article 7 of the DP Law).

The details of the erasure, destruction, and anonymization process is regulated under the Regulation on Erasure, Destruction and Anonymization of Personal Data. In addition, a Guide on Erasure, Destruction or Anonymization of Personal Data has been prepared by the Board to clarify implementation. Notably, data controllers that are required to register with the Data Controllers Registry (VERBİS) must draft a data storage and extermination policy; the mandatory content which has been laid out in the aforementioned regulation.

Decisions regarding Erasure, Destruction and Anonymization of Personal Data

Decision Number	**2018/142**
Board Ruling	Bank is legally obligated to retain data subject's personal data under relevant banking legislation, and, therefore, has a valid legal basis to continue processing the personal data of the data subject.

7. Data Security Measures

Data controllers are obligated to (see, Article 12 of the DP Law):

- prevent unlawful processing of personal data,
- prevent unlawful access to personal data,
- ensure retention of personal data.

A data controller must take all necessary technical and organizational measures to provide appropriate data security in order to fulfill the above listed obligations. Unlike the GDPR, the rights and obligations of a data processor are not specifically regulated by the DP Law, still they are under obligation to ensure data security jointly with data controllers. Within this framework, data processors shall comply with the instructions of the data controller while processing personal data transferred to them, and not disclose such personal data, nor use such data for purposes other than processing purpose determined by the data controller. These obligations shall continue even after the end of their term as data processor.

Considering the importance of special categories of personal data, and the need to secure it accordingly, the Board, in one of its rulings, introduced additional data security safeguards for data controllers dealing with special categories of personal data.

The Digital Transformation Office of the Presidency of Republic of Turkey published a guideline for technical and administrative measures to be taken for the protection of data by the public authorities and key infrastructure organizations, dated 10 July 2020. The guideline, which is alignment with the Board's guideline, contains a variety of detailed and well-established rules for protecting data, and applicable to, among others, internet safety, cyber security of phones, cloud computing applications, crypto applications, compression algorithms. Although the guideline is intended for public authorities and key infrastructure organizations, it is also useful for private entities. It would not be wrong to assume that the Authority, as a public authority, would also follow the guideline and consider the measures prescribed under this guideline when assessing the adequacy of protective measures employed by data controllers.

Decisions regarding Data Security

Decision Number	**2018/10**

This Decision clarified the adequate measures to be taken by data controllers while processing special categories of personal data, and is expected to significantly affect how data controllers handle such data in their daily operations.

Information on "race, ethnicity, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, membership to associations, foundations or trade-unions, health, sexual life, criminal convictions and security measures," and "biometric and genetic data," falls under the term "Special Categories of Personal Data," the processing of which is subject to the measures specified in the decision.

The Decision lists the measures under five categories as follows:

- Policies and procedures
- Employees
- Electronic Systems:
- Physical Filing Systems:
- Transfers

Decisions regarding Data Security

Decision Number	**Principal Decision numbered 2019/308**

Principal decision of the Board, numbered 2019/308, determined that use of certain software, programs, and applications that enable their users to unlawfully gain access to or process personal data such as identity and contact information, by certain professional groups, law firms, and some individuals and organizations operating in finance, real estate consultancy, insurance, and similar sectors violates data security rules under Article 12 of the DP Law.

In this regard, the Board ruled that it will file official complaints before the Prosecutor's Office against those who use such software, programs, and applications, and those acting as data controllers within the scope of the DP Law will be subject to administrative fines regulated under Article 18 of the DP Law.

Decision Number	**2019/269**
Board Ruling	The Board fined Facebook due to failure to take the necessary technical and administrative measures to prevent possible data breaches, and to notify the Board of such breaches.
Decision Number	**2019/ 389**
Board Ruling	The Board decided that a university should adopt certain data security measures for its announcement procedures and should inform data subjects of its processing activities.

8. Data Breach Notification

Data controllers are obliged to notify data subjects and the Board within the shortest possible timeframe, in the event that processed data are collected by parties through unlawful methods. When necessary, the Board may announce such breach on its official website or through other methods it deems appropriate.

8.1 Procedural Details

No statutory details have been envisaged for the data breach notification process, the Board, however, determined the required procedures applicable to breach notification in its decision, dated 24 January 2019, and numbered 2019/10; which requirements can be summarized as follows:

- Data controller shall notify the Board within seventy-two (72) hours, at the latest, from the date he/she learns of a breach, and shall promptly notify the data subject(s) after identifying, using appropriate methods, the person(s) affected by data breach.
- If the data controller cannot with good cause notify the Board within seventy-two (72) hours, it must provide to the Board with the reasons of breach as well.
- Data breach notifications will be made through the standard form (Data Breach Notification Form) announced by the Board.
- In case all of the information requested in the Data Breach Notification Form cannot be provided by the data controller at once, it can provide such information to the Board in phases, without delay.
- Data controller must record the information, effects, and measures taken in relation to the data breach, and make same available for the Board's review, if requested.
- If a data breach occurred in the processing activities of a data processor, it must notify the data controller(s) immediately that data breaches have occurred within their organization.
- In case a data breach occurs within a data controller located abroad, it must notify the Board if the breach meets the following conditions: (i) the consequences of the breach affect data subjects residing in Turkey, and (ii) data subjects in Turkey benefit from the products and services provided by the data controller.
- Data controllers are obliged to prepare a formal data breach response plan, and review it periodically. This plan should include information such as to whom within the organization a data breach should be reported, and who will be held accountable after an assessment of the potential consequences, and charged with providing notice of the breach in accordance with the DP Law.

8.2 Notification Content

The Board's Data Breach Notification Form requests the following information:

- **Information Regarding the Data Controller:** Title/name and address of the data controller and information on the person charged with preparing notice of breach.
- **Information Regarding the Data Breach:** Data controllers should provide detailed information regarding the data breach, such as how it occurred, its source, how and when it was detected, the categories of personal data affected, data subject categories affected, etc.
- **Information Regarding Notification to the Board and Effected Data Subjects:** Data controllers should provide the reasons for not timely notifying the Board (if more than 72 hours have passed since detection and notification of the data breach), when and how it will notify affected data subjects, and the names of any institutions requiring notification.
- **Information Regarding Potential Consequences:** In the event of a data breach, data controller should notify the Board about the possibility of significant adverse consequences to data subjects, as well as internal ramifications.
- **Information Regarding Measures That Have Been Taken Or Will Be Taken After Data Breach:** Data controllers should describe the training given to employees involved in the data breach, technical and organizational measures taken to prevent of data breaches, and technical and organizational measures that will be taken post breach.

8.3 Recommended Measures

In the event of a data breach within data controller, the following steps should be taken:

- All data controllers must have a data breach response plan, and review it periodically.
- Data controllers must have the necessary infrastructure to keep records related to data breaches.
- Upon the detection of a breach, data controllers should shut down all breached systems, and the source of the breach should be investigated.
- When investigating the source of a data breach, the data categories affected, the number of people effected, and the affected data subject categories should be determined.
- Technical and administrative measures should be taken immediately to ensure data security.

- The Board's Data Breach Notification Form should be filled out without delay and, within 72 hours, at the latest, from the time the data controller learned of the breach. It should be kept in mind that notification can be made partially, and data controllers may revise the Data Breach Notification Form after submission to the Board.
- Data controllers should prepare a notification form for notifying affected data subjects.
- After notifying the Board and data subjects, data controllers should take additional technical and administrative measures to ensure adequate data security.

The Board has also published a guideline for filling out the Data Breach Notification Form, and how to use the data breach notification system established by the Board.

In its decision, dated 18 September 2019, and numbered 2019/271, the Board emphasized that the purpose of timely data breach notification is to try to limit the negative consequences to data subjects affected by the breach. In its decision, the Board determined the minimum requirements of a data breach notification to data subjects and stated that data breach notifications to data subjects must be in clear.

plain language, and must include at least:

- The time and date of breach,
- Categories of data (personal data, special categories of personal data) affected by the breach,
- Possible consequences of the breach,
- Measures that have since been taken, or will be taken by the data controller to address the breach and mitigate its consequences,
- The name and contact details of the contact person(s) from whom data subjects may obtain more information about the breach, or some other means of communication, such as the data controller's website, call center, etc.

Decisions regarding Data Breach Notification	
Decision Number	**2019/104**
Board Ruling	The Board fined Facebook for failing to notify the Board of a data breach. The breach was detected on 19.09.2018, but no notification was given; and notification of a data breach which occurred between 13.09.2018 - 25.09.2018, wasn't given until 17.12.2018.
Decision Number	**2019/222**
Board Ruling	The Board fined Dubsmash, Inc., for notifying the Board nineteen days after a data breach.
Decision Number	**2019/269**
Board Ruling	The Board fined Facebook for failure to notify the Board of a data breach.

9. Data Controllers Registry System ("VERBİS")

VERBİS is an online registration system on which data controllers record their data processing activities. In principle, all data controllers are required to register with VERBİS before processing personal data (see, Article 16 of the DP Law), however, the Board may, in its discretion, grant exemptions.

In this regard, the Board issued decisions granting exemptions from the VERBİS registration requirement to certain professional groups, associations, and political parties. The Board has also granted a general exemption to local data controllers whose:

- Annual number of employees is less than 50, **OR**
- Annual balance is less than TRY 25 million.

A local data controller with employees or revenue in excess of the foregoing must register with VERBİS unless they fall within another exception, or one is granted by the Board on other grounds.

Notably, data controllers abroad processing data from Turkey must without exception register with VERBİS.

The deadline for the registration has been extended by the Board three times. The first deadline was determined as 30 September 2019, for the controllers with more than 50 employees, or annual revenue exceeding TRY 25 million, and/or data controllers residing in or registered outside of Turkey. However, that deadline was first pushed to 31 December 2019, then to 6 June 2020, and, most recently, to 30 September 2020.

Currently, the following registration deadlines apply:

- **30 September 2020,** for data controllers with more than 50 employees, or whose annual revenue exceeds TRY 25 million, and/or data controllers residing in or registered outside of Turkey.
- **31 March 2021**, for the data controllers with less than 50 employees, and annual revenue exceeding TRY 25 million, and which is materially engaged in processing special categories of personal in the ordinary course of business.
- **31 March 2021,** for public entity data controllers.

On 1 October 2020, the Board announced publicly on its official webpage that there were data controllers who, as of the date of the announcement, failed to register with VERBİS, or failed to complete certain notification after submitting their registration. The Board, pursuant to its decision, dated 1 October 2020, and numbered 2020/760, notified data controllers contemplated by the announcement that, in consideration of difficulties resulting from COVID-19 which may have rendered them unable to timely register with VERBİS, they are granted a final opportunity, not, however, a postponement, to register immediately.

Below is an outline of the steps to be taken by the data controllers abroad in registering with VERBİS. The initial step in the registration process is creating a VERBİS user account which includes specifying a contact person for registrant.

9.1 Preparation of a Data Inventory for Personal Data Processed in Turkey

Data controllers must prepare a processing inventory for all data processed in Turkey. The inventory must contain all information required by the DP Law, must be kept up-to-date, accurate, lawful. Data controllers must provide notice via VERBİS of changes in data inventory within seven days of such change. A data inventory should include at least the following information:

- Identifying information (including, the address of the data controller or its representative)
- Data categories processed by the data controller
- Purposes of processing for each data category
- Maximum retention period for each data category
- Data subject groups for each data category
- Information on whether selected data categories are transferred abroad
- Data transferee groups to which the personal data is transferred
- Data security measures implemented by the data controller

It should be noted, that VERBİS records are fully accessible to the public.

9.2 Appointment of A Data Controller Representative

The registration process for data controllers abroad is more complex, and requires appointment of both a data controller representative (Turkish legal entity or real person) and contact person (Turkish real person).

It should be noted, that local data controllers are not required to appointment a representative. They are however advised to do so in order to ensure focused and appropriate handling of data protection matters.

A data controller abroad should resolve to appointment a representative in Turkey. Such resolution must be written, notarized, and apostilled, or otherwise appropriately legalized. The appointed representative must complete the registration form available online and submit it to the Board, together with the legalized resolution to appoint a representative in Turkey.

The representative then appoints a contact person. It is advisable to register using a registered email address ("**KEP**"[2]) in order to complete registration process faster. If the Turkish representative does not have registered email address, one can be obtained, or, if not possible, all documents may be delivered to the Board at its published address via registered mail.

All data controllers must specify in VERBİS a contact person who must be a Turkish citizen, and such appointment must be the sole appointment of that person in VERBİS.

9.3 Appointment of a Contact Person

Data controllers are required to appoint a contact person responsible for communicating with the Board, appropriately list that person in VERBİS, and all VERBİS notifications will be transmitted thereto via the e-government account (E-devlet) thereof. Rules for the appointment of a contact person are as follows:

- Contact person must be a real person who is a Turkish citizen residing in Turkey.
- Contact person must be over the age of eighteen.
- Contact person cannot be the contact person for multiple data controllers simultaneously.
- A data controller cannot have multiple contact persons at any one time.
- A data controller may change its contact person at will.
- A data controller may choose to designate an employee or a third party outside of the organization as contact person.

The contact person is charged with submitting data inventories and completing VERBİS registration.

[2] KEP is an electronic mail address obtained from companies authorized to provide registered email service. Please see the link to the Information and Communication Technologies Authority's list of authorized providers https://www.btk.gov.tr/kayitli-elektronik-posta-hizmet-saglayicilar

If the data controller does not have KEP, it must apply for one with an authorized service provider, and provide the following documents:

- Application form
- Commercial activity certificate including data controller's MERSİS number
- Signature circular of data controller
- Proxy, if the application will be submitted by a real person who is not the legal representative of the data controller
- Appropriate identification papers for the actual applicant

The KEP address must be active and functioning.

E. Sanctions

1. Administrative and Criminal Sanctions

Failure to comply with the DP Law will result in serious consequences which, depending on the nature of the non-compliance, may include, among others, administrative fines (see, Article 12 of the DP Law), and criminal sanctions (see, Article 135-140 of the Turkish Criminal Code, numbered 5237).

If an administrative sanction is imposed, the subject of the administrative penalty will be the legal entity itself, in its capacity as data controller. As for the criminal sanctions, in Turkey, unlike some other jurisdictions, merely legal entities cannot be held criminally liable. Accordingly, criminal liability would attach to executives of the data controller. Also, safety measures may be imposed on legal entities.

Allegations of DP Law violations may be brought to the attention of public prosecutors under the Turkish Criminal Code, or under the DP Law itself, and civil actions can be filed in the general courts for violation of personal rights.

1.1 Administrative Sanctions

Non-compliance with certain DP Law requirements will trigger administrative sanctions (see. Article 18 of the DP Law) . Accordingly, for:

- Violation of the obligation to inform will be imposed with an administrative fine between TRY 9.384,00 – TRY 196.689,00.
- Violation of the obligation with data security will be imposed with an administrative fine between TRY 29.503,00 – TRY 1.966.862,00.
- Violation of the compliance with the Board's decision will be imposed with an administrative fine between TRY 49.172,00 – TRY 1.966.862,00.
- Violation of the registration obligation to VERBİS will be imposed with an administrative fine between TRY 39.337,00 – TRY 1.966.862,00.

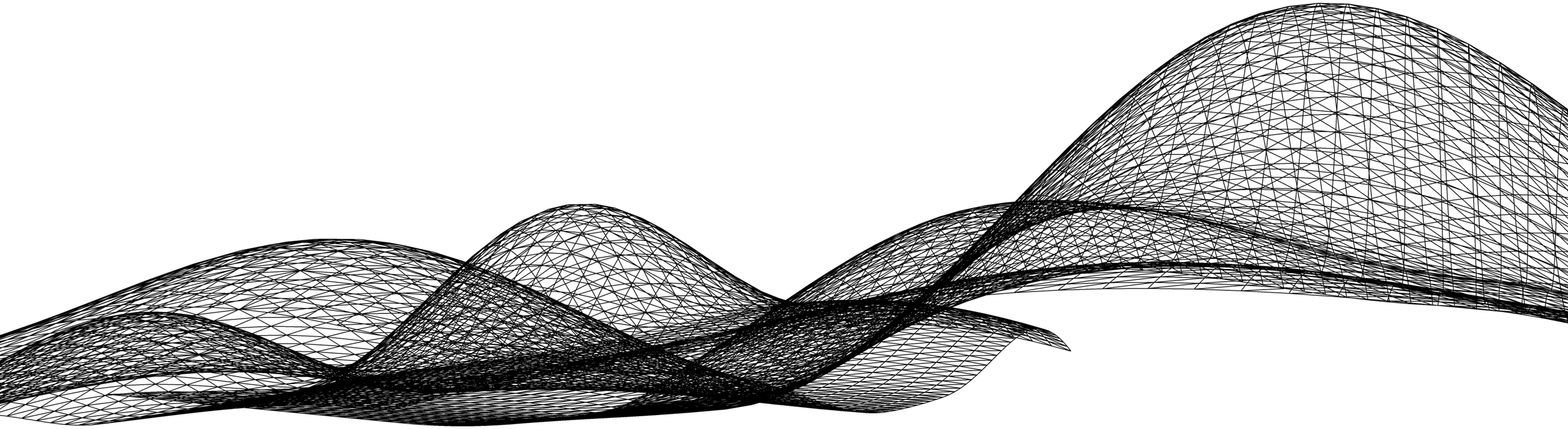
1.2 Criminal Sanctions

Under the Turkish Criminal Code:

- Unlawful recording of personal data is punishable by imprisonment for 1 to 3 years. If the personal data unlawfully recorded relates to race, ethnic origin, political and philosophical views, sexual life, health, membership in a trade-union, then by imprisonment for up to 4,5 years.
- Illegally obtaining, transferring, and disseminating personal data is punishable by imprisonment for 2 to 4 years; provided, however, that if committed (i) by a public official in misuse of power, or (ii) by an individual misusing benefits or privileges of a profession or trade, then punishable by up to 6 years imprisonment.
- Failure to destroy personal data after expiration of the applicable statutory retention period is punishable by imprisonment for 1 to 2 years; provided, however, that where such failure is, due to the nature of the data, within the purview of the Turkish criminal law, then punishable by up to 4 years imprisonment.

MOROĞLU ARSEVEN

II. ANALYSIS ON BOARD ACTIVITY



A. Overview

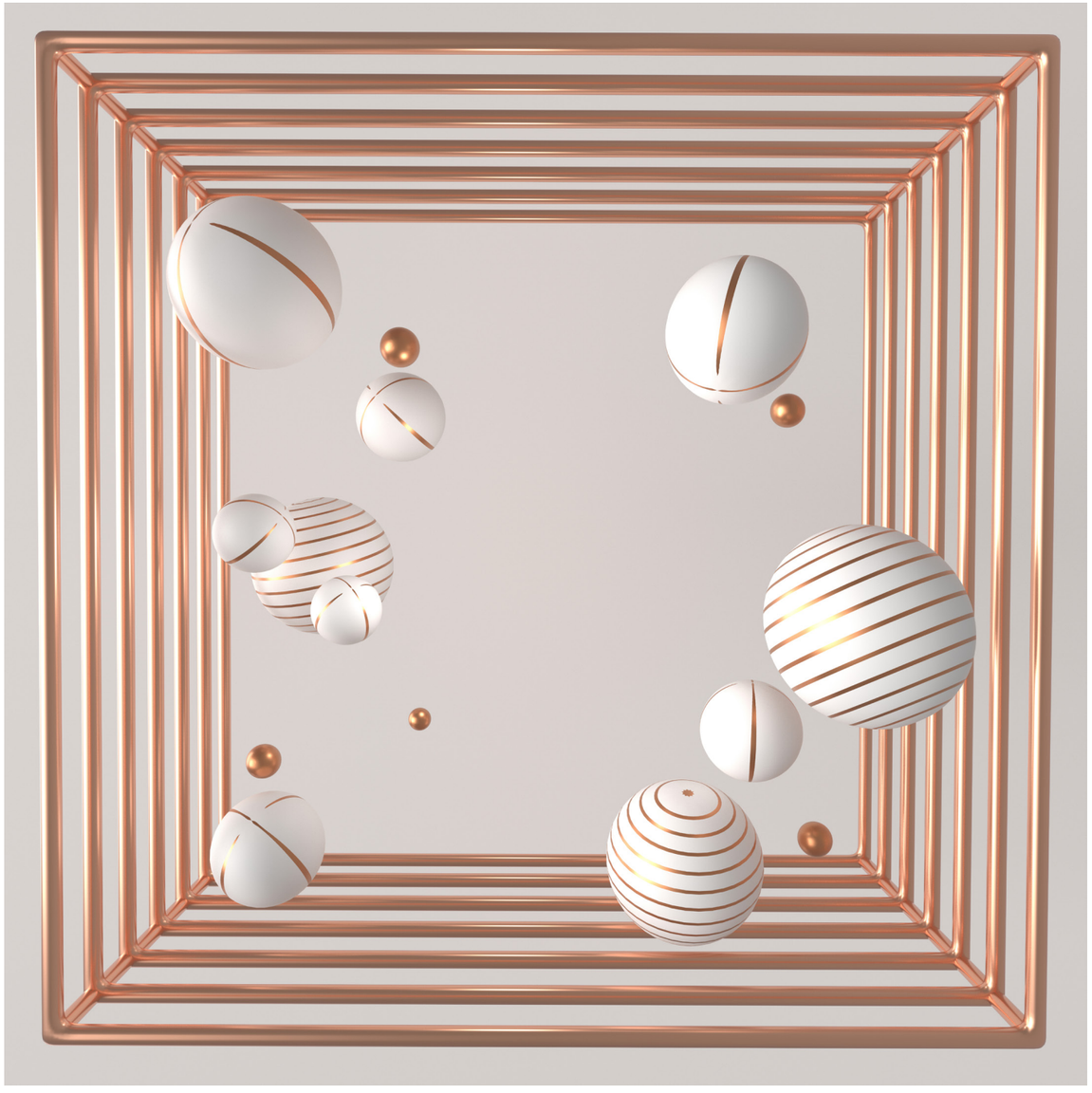
As an independent decision making body under the the DP Law, the Board has, since 2017, issued many decisions; some of a regulatory nature, others secondary legislation to the DP Law, yet most deal with enforcement of the DP Law.

Apart from other regulatory authorities in Turkey such as the Competition Board and Capital Markets Board, the Board is not under any obligation to publish its decisions, and it is within its discretion whether a particular decision will be published and in what form, and whether and to what extent redactions are necessary prior to publishing.

To date, the Board has published, in whole or in summary, a total of 85 decisions. Six of them are principal decision, and their full texts are available on the Board's website.

Notably, with respect to the remaining 75 decisions, which pertain to individuals, the Board released summaries to the public containing limited detail. With little exception, the summaries do not contain the name of the subject individuals. When comparing older summaries to more recent ones, there seems to be a trend toward releasing more detailed summaries, including even the names of data controllers

In addition, and pursuant to Article 12/5 of the DP Law, the Board in its discretion publishes data breach notifications on is website to notify data subjects potentially impacted by a data breach, 67 of which have been published to date. These notifications are usually summaries of the information received by the Board from the breached data controller.



MOROĞLU ARSEVEN

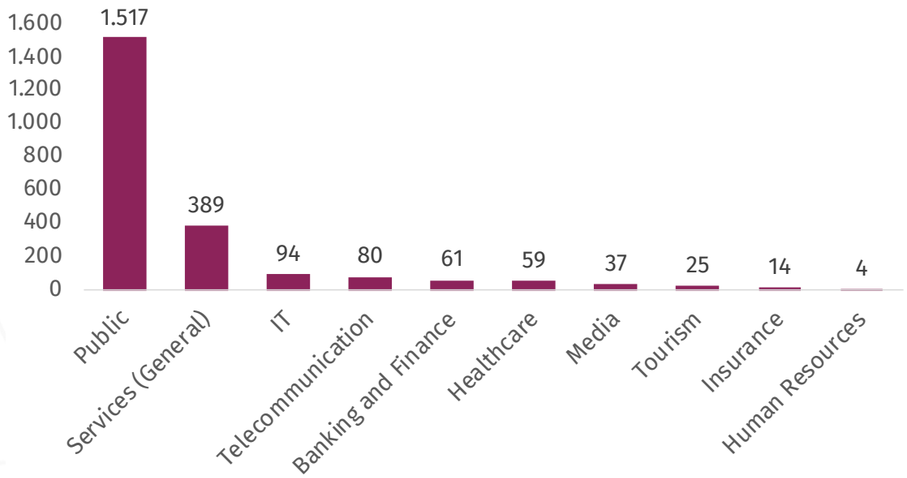
MOROĞLU ARSEVEN

B. Key Numbers from the Board

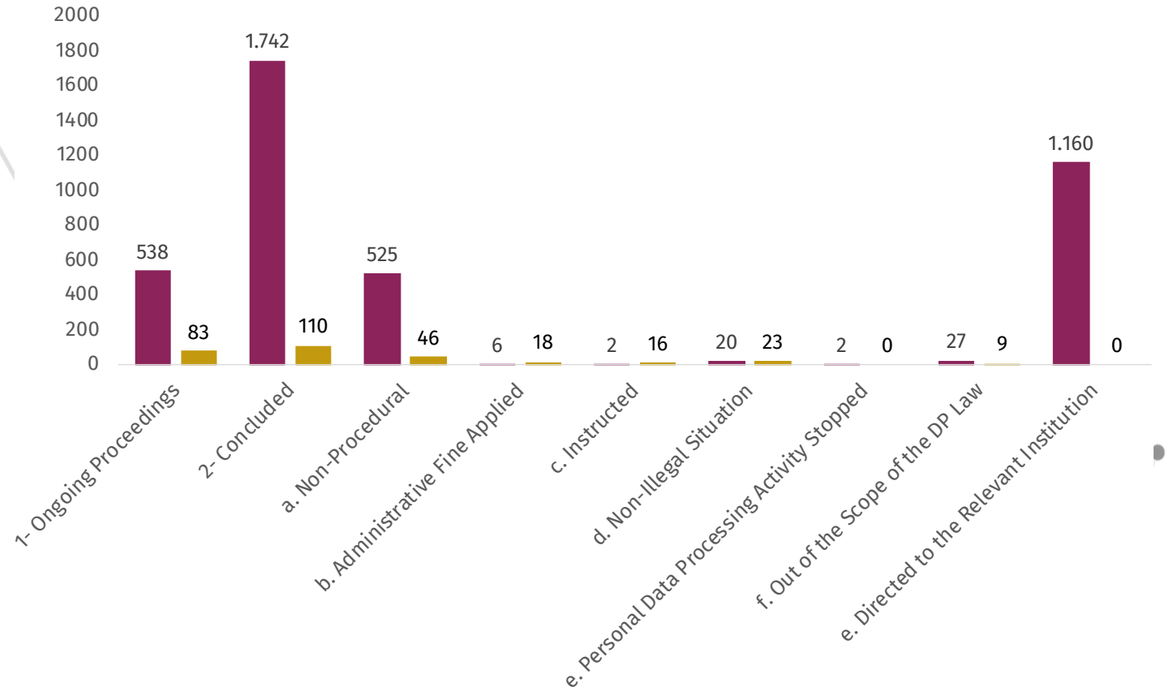
The Board has published its Activity Report for 2019 ("**Report**"). The official numbers disclosed in the Report are as follows:

1. Complaints

1.1 Complaints by Sector

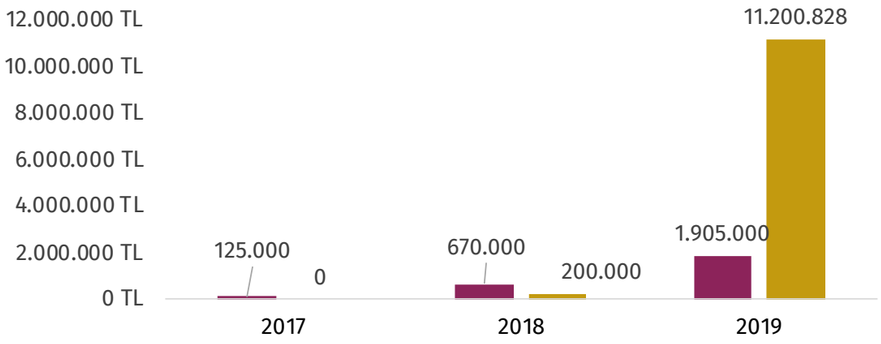


1.2 Complaint Statistics



2. Board Decisions

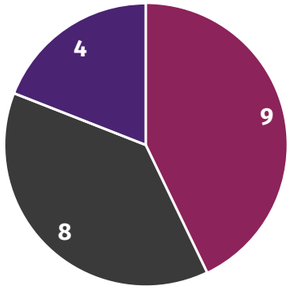
2.1 Sanction Statistics



2.2 Sanction Facts

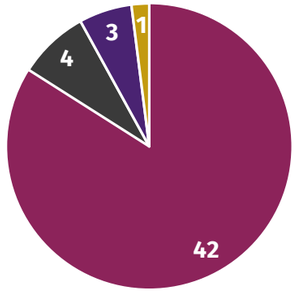
- administrative fines for failure to take all necessary technical and administrative measures to prevent unlawful processing,
- administrative fines for failure to notify the Board and data subjects in a reasonable time of unlawful processing of personal data,
- administrative fines for failure to fulfil the Board's instructions and orders to remedy violations,
- administrative fines for failure to comply with general data protection principles;,
- administrative fines for failure to comply with Article 11 which regulates the rights of data subjects.

Published Decisions by Sector



- Banking and Finance
- IT and Telecommunication
- Healthcare

Published Decisions by Article



- Fines for Non-Compliance with Data Security Rules - Art. 18/1(b)
- Disciplinary provisions to public institutions / public authorities decisions – Art. 18/3
- Fines for of Non-compliance with the Board's decisions – Art. 18/1(c)

TOP ADMINISTRATIVE FINES

As shown in the chart below, IT and Media sectors have taken the lead with respect to both number and total of fines imposed in the top 5 notable decisions. It also appears that fineslaws in information systems are the main reason for the data breaches in four of them, rather than administrative fineslaws, accompanied by failure to timely notifying the Board. In one decision, regarding factoring companies and Risk Center data, employees of the data controller were responsible for the breach. Notably, the information systems of banks and financial institutions, which are strictly regulated and regulary audited, are generally very secure.

No	Name of Data Controller	Industry	Violated Article	Total Fine	Date
1	Facebook	Information Technology and Media	Article 12/1, Article 12/5	TRY 1.650.000	11.04.2019
2	Facebook	Information. Technology and Media	Article 12/1,Article 12/5	TRY 1.550.000	18.09.2019
3	Marriott International Inc.	Tourism	Article 12/1, Article 12/5	TRY 1.450.000	16.05.2019
4	Dubsmash Inc.	Information Technology and Media	Article 12/1, Article 12/5	TRY 730.000	17.07.2019
5	Clickbus Seyahat Hizmetleri A.Ş.	Transportation	Article 12/1, Article 12/5	TRY 550.000	16.05.2019
6	Cathay Pasific Airway Limited	Transportation	Article 12/1, Article 12/5	TRY 550.000	16.05.2019
7	Not indicated	Tourism	Article 12/1, Article 12/3, Article 12/5	TRY 500.000	27.08.2019
8	Not indicated	Gym	Article 12/1, Article 12/3 Article 12/5	TRY 225.000	27.02.2020
9	Not indicated	Banking and Finance	Article 12/1	TRY 210.000	06.02.2020
10	Not indicated	Electronics	Article 12/1, Article 15/5	TRY 200.000	14.02.2019 05.03.2019
11	S Şans Oyunları A.Ş.	Information Technology and Media	Article 12/1, Article 12/5	TRY 180.000	27.08.2019
12	Not indicated	Technical Service	Article 12/1	TRY 150.000	14.02.2019
13	Not indicated	Media	Article 12/1	TRY 125.000	09.12.2019
14	Not indicated	Information Technology and Media	Article 11, Article 12/1 Article 10	TRY 110.000	27/01/2020
15	Not indicated	Banking and Finance	Article 4/2, Article 12/1	TRY 100.000	18.09.2019
16	Not indicated	Airlines	Article 12/1	TRY 100.000	01.10.2019
17	Not indicated	Insurance	Article 12/1	TRY 100.000	07.11.2019
18	Not indicated	Banking and Finance	Article 12/1, Article 12/5	TRY 100.000	26.11.2019

Article 12/1: Failure to take all necessary technical and administrative measures to prevent unlawful processing
Article 12/3: Failure to audit compliance with the DP Law within the organization
Article 12/5: Failure to notify the Board and data subjects in a reasonable time of unlawful processing of personal data
Article 15/5: Failure to fulfil the Board's instructions and orders to remedy violations

C. Notable Decisions

1. Decisions Regarding Adequate Technical Measures

Decision No: 2019/104
Sector: Information Technology and Media

The case involved an API bug on Facebook. Facebook's internal team discovered a photo API bug that affected people who used Facebook Login, which granted permission to third party apps to access their photos. As a result, some third party apps might have had access to a broader set of photos than usual for 12 days, between September 13 and September 25, 2018. The Board considered the length of breach, together with Facebook's unresponsiveness, as prima facie evidence of lack of adequate technical and administrative data protection measures. In addition, since Facebook was unable to determine the extent of the breach, the board found it deficient in its data flow detection. The breach affected 6,8 million people globally, with 300.000 in Turkey; and Facebook never notified the Board.

The Board imposed a record fine of TRY 1.650.000 which Facebook has yet to pay.

Decision No: 2019/269
Sector: Information Technology and Media

On 25 September 2018, Facebook representatives informed the Board by email that a data breach had occurred caused by the complex interaction of multiple bugs related to different Facebook features. Between 14 September 2018 and 28 September 2018, attackers were able to access user personal data using access tokens generated as a result of the interaction of multiple bugs in three separate features of Facebook called "View As," "Video Upload Tool," and "Happy Birthday Videos."
280.959 users of Facebook in Turkish language were affected by the breach.

Considering that Facebook should have detected and fixed the offending bugs in pre-launch testing, the Board found Facebook to have failed to take necessary administrative and technical measures to protect user personal data. Furthermore, considering that the vulnerability continued for 14 months, between 21 July 2017 and 27 September 2018, without a timely, internal, ameliorative response, the Board found that Facebook failed to take necessary administrative and technical measures to protect user personal data.

Decision No: 2019/143
Sector: Tourism

The case involved unauthorized access to the customer database of Starwood Hotels, a wholly owned subsidiary of Marriott International.

The breach lasted from 2014 to 2018. The attacker having installed a trojan horse on the web server was able to assume control of it remotely. Taking into consideration the four years breach duration, number of individuals affected, the nature of the accessed data, the overall severity of the breach, and lack of timely notice, the Board imposed an administrative fine of TRY 1.450.000 on Marriott.

Decision No: 2020/191, 2020/192, 2020/193, 2020/194
Sector: Banking and Finance

Upon receiving notice of credit score increases in credit checks performed by certain Risk Center members, the Board opened an investigation.

The Board discovered that employees of four factoring companies illegally used Risk Center data to check credit scores and access other information which they then transferred to third parties. The Board found that adequate administrative and technical measures to prevent the breach were not taken, no notification was made to the Board, and imposed an administrative fine of TRY 1.400.000. (for each one).

Decision No: 2020/286
Sector: Information Technology and Media

The decision relates to unauthorized access to a game company's cloud systems containing user data. The unauthorized access was detected via the company's log records.

The Board found that the attacker's ability to access to the cloud systems was a sign of insufficient vulnerability testing, and that preventative technical measures were employed only after the breach occurred, and no notification was made to the Board.

Accordingly, the Board imposed an administrative fine of TRY 1.100.000.

2. Decisions Regarding Transfer of Personal Data

Decision No: 2020/559
Sector: Automotive

Upon a data subject's complaint about receiving an unsolicited marketing message from the data controller, the Board opened an investigation. The Board discovered that the data controller used a web-based messaging system to transfer personal data to a cloud database located in an EU member country for text message marketing campaigns. The central issue, therefore, was whether the data was processed and transmitted in compliance with the DP Law.

The Board, citing Article 12 of Convention 108, stated that a contracting state shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization trans-border flows of personal data going to the territory of another contracting state. That provision, however, does not remove a contracting state's right to regulate data processing activities under local law, or to enact rules or restrictions governing data transferring abroad. The Board stated that being a party-country to Convention 108, though considered by the Board, is not itself sufficient to render a country with adequate level of protection for personal data transfer.

Although the data controller when it performed the cross-border transfers in reliance on Convention 108 believed them to be in compliance with the DP Law, they were not. Convention 108 notwithstanding, the requirements of the DP Law were not met, and the data transfer was unlawful

Decision No: 2020/173
Sector: Information Technology and Media

This e-commerce case involved a cross-border transfer of personal data without explicit consent of the data controller.

The relevant e-commerce website's privacy notice provided that by visiting the website data subject accepts the conditions contained in the privacy notice, and data subject would be notified regarding transfer of personal data, and have the opportunity to opt out.

The Board held that (i) explicit consent cannot be incorporated into a general privacy notice, and must be obtained before transfer of personal data, (ii) providing an opportunity to opt-out after personal data is transferred is unlawful, and (iii) explicit consent must be informed, which requires, in this case, among other things, a clear disclosure of the cross-border nature of the transfer. Accordingly, no explicit consent was obtained, and the transfer was unlawful.

Decision No: 2019/157
Sector: N/A

The Board, upon an opinion request, delivered and published a decision regarding the use of email services. According to the Board, using infrastructure of a foreign based email service (which does not designate a local server for Turkish users) would result in the data being kept in data centers all around the world. In this case, the principles regarding cross-border data transfer must be followed in order to transfer personal data using such email services.

Decision No: 2020/26
Sector: Legal Services

Text messages sent to a data subject's relative regarding execution proceedings initiated against the data subject. The data controller was a law office that had initiated legal proceedings to collect from data subject a client bank's receivables. The data subject received phone calls and text messages from the law office regarding the execution proceedings. However, the text messages were also sent to a relative of the data subject whose contact information was obtained through a third party. The Board found the data transfer between the data controller and the third party unlawful and imposed an administrative fine on the data controller-law office.

Decision No: Stated in Board's Guideline[5]
Sector: N/A

A document containing personal data of a data subject was sent to a third party with the same first and last name. The Board opened an investigation. According to the Board, such an incident demonstrates a flaw in the systems of the data controller when authenticating the identity of data subjects. The investigation also revealed that the data subject's personal data was searched several times in the system by an employee not at the request of the data subject. Consequently, an administrative sanction was imposed on the data controller.

Decision No: 2019/389
Sector: Education

The Board, upon an opinion request, delivered and published a decision regarding announcing applicant results online. The university requesting the opinion planned to announce on its website decisions on academic job applications, and sought the Board's approval. According to the Board, the results must be open only to the candidate and must be accessible with identification authentication. If the results are to be published on the website, they should be masked such that no association is possible between an applicant's personal information and job application (for example, by revealing only the initials of the first name and the last name, and the first two and the last two numbers of their national identification number), and the university, as data controller, must provide appropriate notice to the data subjects.

[5]https://www.kvkk.gov.tr/Icerik/5416/Kisisel-Veri-Guvenliginin-Saglanmasi-Amaciyla-Uygun-Guvenlik-Duzeyini-Temin-Etmeye-Yonelik-Gerekli-Idari-ve-Teknik-Tedbirlerin-Alinmamasi

3. Decisions Regarding Special Category Personal Data

Decision No: 2020/649
Sector: N/A

The Board, upon an opinion request, delivered and published a decision regarding biometric signature, which includes, among other things, the way one walks, types on a keyboard, applies pressure to or taps a smart device, and drives a car. In cases where there is no express consent, biometric data can only be processed if prescribed by law; and such provision of law should be clear enough to leave no grounds for doubt.

To create a biometric signature, requisite data components are obtaining using specialized devices. The gathered data is then inseparably linked to a signed document. Since biometric signatures, and the methods for obtaining them, are not standardized, they are not legally equivalent to wet signatures.

In that regard, the Board noted that provisions Turkish Code of Obligations ("**TCO**") regulating written contracts and signatures apply to traditional (wet-ink) and electronic signatures; and to interpret such provisions otherwise would give the impression, though incorrect, that biometric signatures are clearly prescribed by law and in accord with the principle of data minimization. Furthermore, the Board concluded that a biometric signature constitutes biometric data and, therefore, is to be considered among special categories of personal data which can only be processed with explicit consent of the data subject, unless otherwise provided under applicable law.

Decision No: 2019/81
Sector: Health and Fitness

The decision concerns the identification authentication method of two gyms, including the use of palm prints to identify and authenticate members as they entered.

The Board considers one's palm and its print to be biometric data falling under the rubric of special category of personal data. Since the proportionality principle in processing personal data requires data minimization. With respect to special category personal data, if equivalent results can be achieved without its processing, then to do so would violate the DP Law.

In the present case, although the data controllers claimed to have received explicit consent of the data subjects for palm print authentication, because such consent was compulsory the Board concluded that even if explicit consent was given, it was invalid and the data processing unlawful. The Board imposed an administrative fine and required the deletion of the palm print biometric data.

4. Decisions Regarding Explicit Consent and Information to Inform

Decision No: 2018/90
Sector: N/A

A data controller accepted job applications on its website. Registering with the site was a prerequisite to applying. Applicants failing to complete the registration were unable to apply. The registration form included a compulsory tick box for explicit consenting to and accepting the site's general privacy notice.

The Board held that the tick box consent was insufficient under the DP Law, and going forward, registered data subjects must be given adequate notice of data processing activity involving their personal data. Furthermore, the data controller prove that it utilized separate mechanisms to inform data subjects and to obtain explicit consent therefrom. Accordingly, a single tick box was inadequate and unlawful.

Decision No: 2019/82
Sector: Grocery

The Board reviewed a grocery store's loyalty program in response to complaints about an explicit consent requirement for membership.

The Board found that while the loyalty program presented several benefits, discounts in particular, to its members, non-member shoppers could purchase the same products, albeit without member only discounts, without joining. Explicit consent is not, therefore, a prerequisite to shopping at the store. Although membership, and explicit consent, provides data subjects with more advantageous purchase opportunities, because it is optional, it is lawful.

Decision No: 2019/206
Sector: N/A

A data controller providing online services required visitors to register before they could access site content and services. Registration included a privacy statement containing a compulsory tick box for explicit consent. Since the data controller required explicit consent to access the site, and because it was requested via a tick box on the general privacy statement consent form, the Board found it invalid and unlawful.

The data controller offered explicit consent as the sole legal grounds for processing personal data. In response, the Board noted that if legal grounds other than explicit consent apply, data controllers should base their activities thereon and to the exclusion of explicit consent.

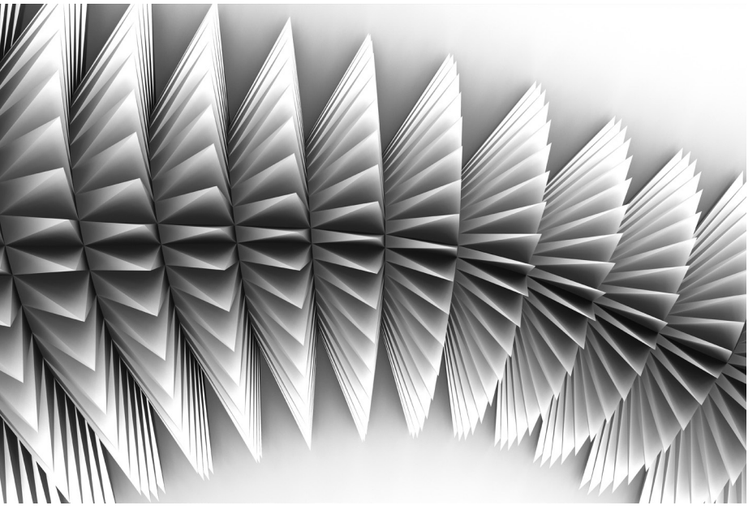
Decision No: 2019/122
Sector: Banking and Finance

The decision concerned a data controller's privacy notice. The data controller asserted that certain data processing activities were permitted under Articles 5 and 6 of the DP Law. The privacy notice was silent regarding same. The Board held that a data controller must specifically and expressly inform the data subject explicitly of legal ground(s) for processing, and should refrain from using ambiguous phrases – e.g, purposes, such as, et cetera - which are inappropriately open-ended.

5. Decisions Regarding Application to the Data Controller

Decision No: 2019/296
Sector: Telecommunications

The decision concerned a data controller's refusal of a data subject's application, submitted via data controller's website, because data controller was unable to authenticate the identity of the data subject; and that then directed the data subject to submit an application by sending the same form through a notary or via registered email for of identity authentication. The Board ruled that the Application Communiqué prohibited data controller from restricting or reducing its application methods because same are misleading and impose financial burdens on data subjects in violation of the DP Law or the Application Communiqué.



Decision No: 2019/294
Sector: Air Transportation

The concerned an airline company requesting a hard copies of a data subject identification documents when changing their loyalty program username and password. According to the Board, although requesting additional information for authenticating the identity of the applicant is not inappropriate, hard copies of identification documents contain special categories of personal data, such as blood type and religion, and therefore can only be processed if clearly prescribed by law. In the present case, the processing was overly extensive and unlawful.

As shown in the chart below, IT and Media sectors have taken the lead with respect to both number and total of fines imposed in the top 5 notable decisions. It also appears that flaws in information systems are the main reason for the data breaches in four of them, rather than administrative flaws, accompanied by failure to timely notifying the Board. In one decision, regarding factoring companies and Risk Center data, employees of the data controller were responsible for the breach. Notably, the information systems of banks and financial institutions, which are strictly regulated and regulary audited, are generally very secure.

D. Data Breach Notifications

As part of the breach notice obligation set out Article 12 of DP Law, the Board has published 67 data breach notifications since 4 May 2018; and imposed fines on 4 data controllers without publishing associated breach notifications.

For its first decisions of year 2018, the Board published only the grounds for its decision to impose an unspecified fine on a data controller. No information whatsoever regarding the data breach was provided. After that case, the Board, in subsequent decision publications, began providing more detailed information regarding the data breach. Recent data breach notifications published by the Board have generally contained the following information:

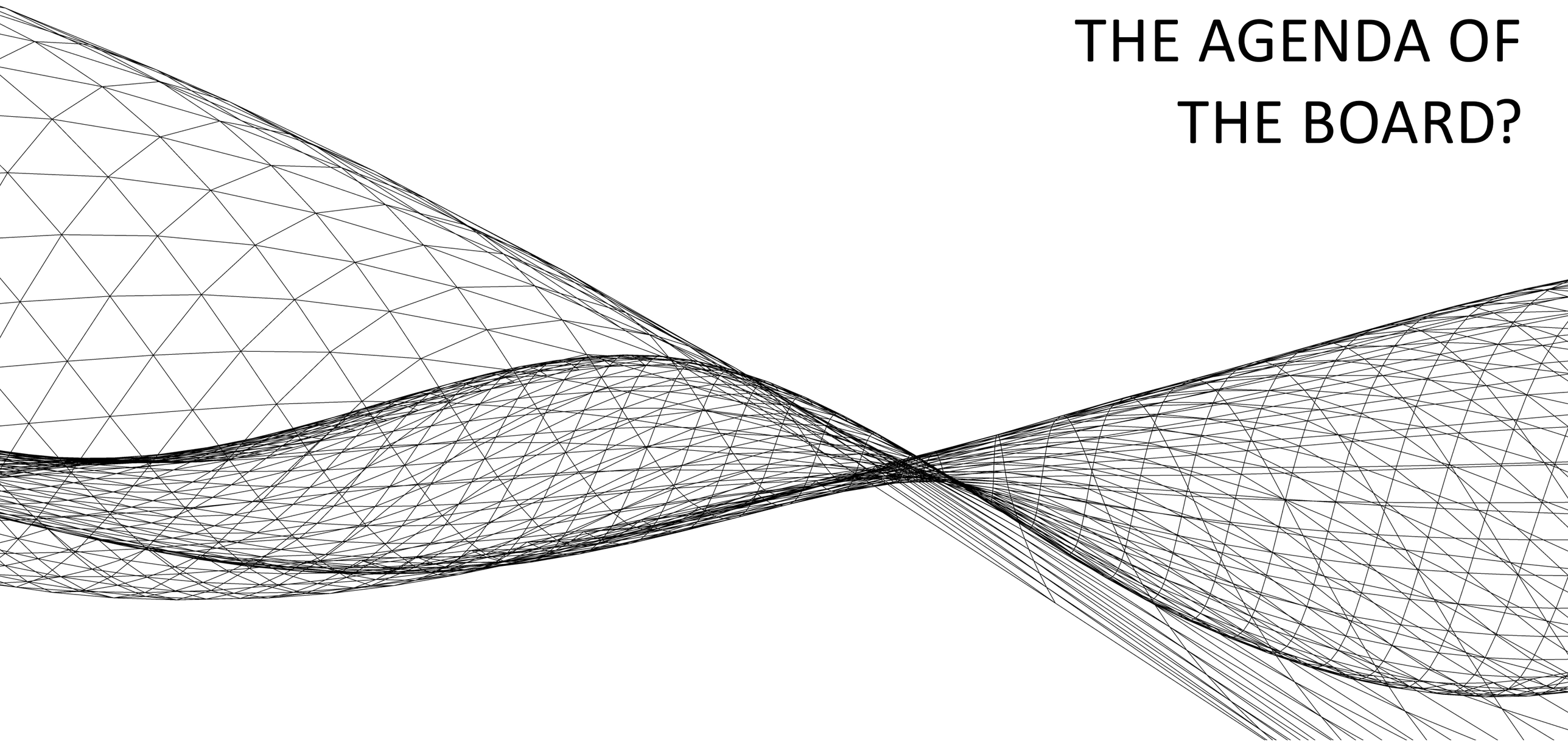
- How and when was the data breach was detected by the data controller. Summary of how the data breach occurred and which systems were affected.
- When notification to the Board was made.
- How many data subjects in Turkey were affected, and which data categories and data subjects were affected?
- Measures taken by the data controller after the data breach.
- How individuals can learn if their personal data is affected, and if so, how to get more information.

Remarkable Points of Data Breach Notifications

- The Board imposed an administrative fine of approximately TRY 7.000.000 on 8 data controllers.
- The Board imposed the highest single administrative fine ever on Facebook in the amount of TRY 1.650.00 for a data breach. The administrative fine imposed on Marriott International, Inc. totaled TRY 1.450.000 and the second largest single fine to date.
- The Board published data breach notifications of 7 data controllers located outside Turkey.
- The table below shows the breakdown by sector of data breach notifications published by the Board to date.

Sector	Number of Decisions
Car Rental Services	15
Technology – Media (Social Media, Mobile Applications, etc.)	9
Banking	5
Tourism (Travel Agencies, Airlines, Hotels, etc.)	5
Other	5
Transportation	2
Retail	2
Telecommunications	1
Public Institutions	1
Pharmaceutical	1
Insurance	1

III. WHAT IS ON THE AGENDA OF THE BOARD?



A. 11th Development Plan

Paragraph 479.1 of the 11th Development Plan of the Presidency of the Republic of Turkey for the years 2019 to 2023 ("**11th Development Plan**") explained that the DP Law is expected to be updated based on the GDPR. Accordingly, several concepts of the DP Law are expected to be altered by taking into consideration the GDPR.

As in the GDPR, the scope of the DP Law may be extended to apply to all data processing activities targeting or tracking Turkish domiciled real persons. New categories of rights of data subjects may be introduced in new amendments, such as right to restriction and to data portability. There may also be changes to the calculation method for administrative fines. Instead of fixed and capped amounts, the legislation may adopt a calculation method based on data controller revenue.

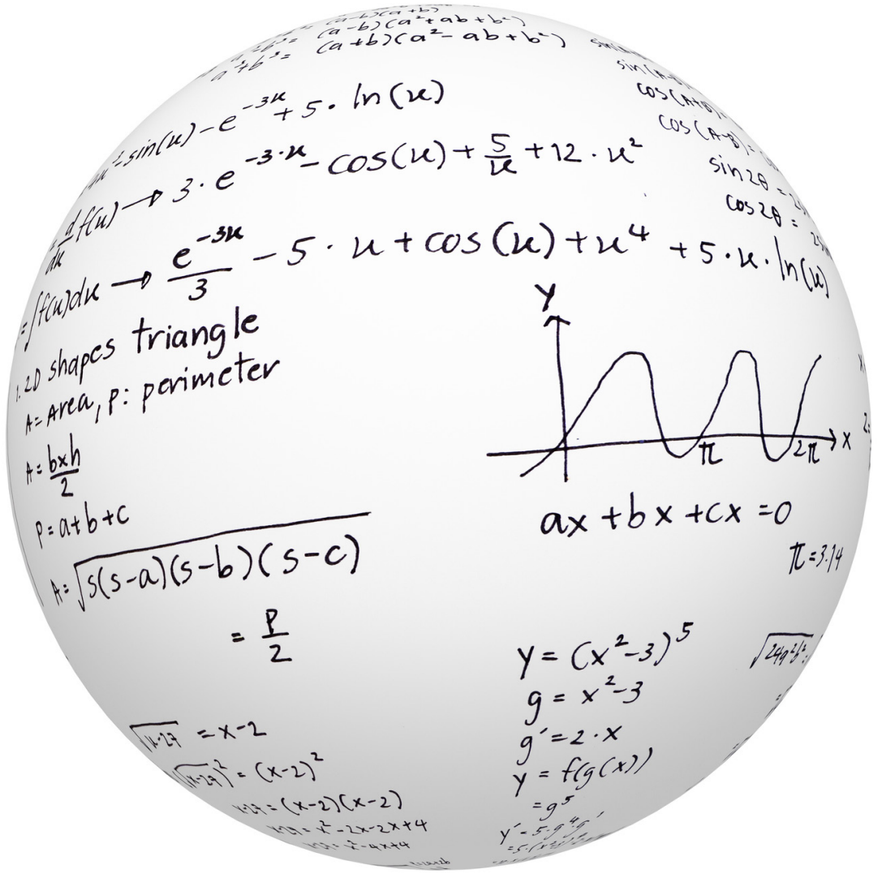
Aside from these, new concepts such as "data protection officers," "data processing records," and "data protection audits" may be introduced in new amendments as well as "privacy by default," "privacy by design," and "joint data controllers."

Lastly, it can be expected that data protection prior to processing will be strengthened through data protection impact assessments and prior consultation with the Board.

B. EU Progress Report

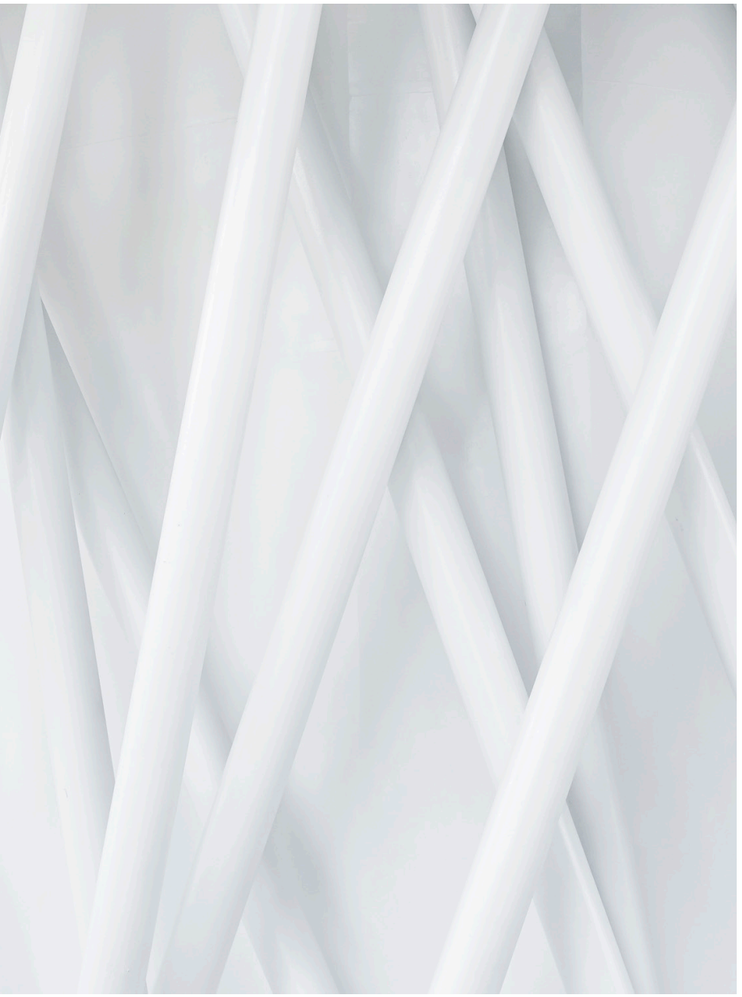
In the European Commission's 2020 Progress Report on Turkey, dated 6 October 2020, the main expectancies with respect to protection of personal data are explained as the harmonizing of the DP Law with the GDPR, and ensuring the independence of the Authority. Furthermore, Turkey is expected to address the EU's concerns regarding independence of the Authority and exceptions for law enforcement under the DP Law. It was further noted that the amendment protocol to Convention 108 has yet to be signed by Turkey.

It is expected that harmonizing the DP Law with the GDPR will alleviate these concerns. As explained in the 11th Development Plan, amendments to the DP Law based upon the GDPR are planned which will provide a data protection regimen more in line therewith.



IV. DEVELOPMENTS EXPECTED IN SHORT TERM

A. Cross-Border Transfers



As explained under the Section I.D.4 hereinabove, in order for cross-border data transfers to be legitimate, a data subject's explicit consent is necessary. However, explicit consent is not required if the receiving party is domiciled in a country with adequate level of protection or adequate protection is undertaken by the receiving party and the data controller. Lastly, the BRC is also available for data transfers between intracompany groups.

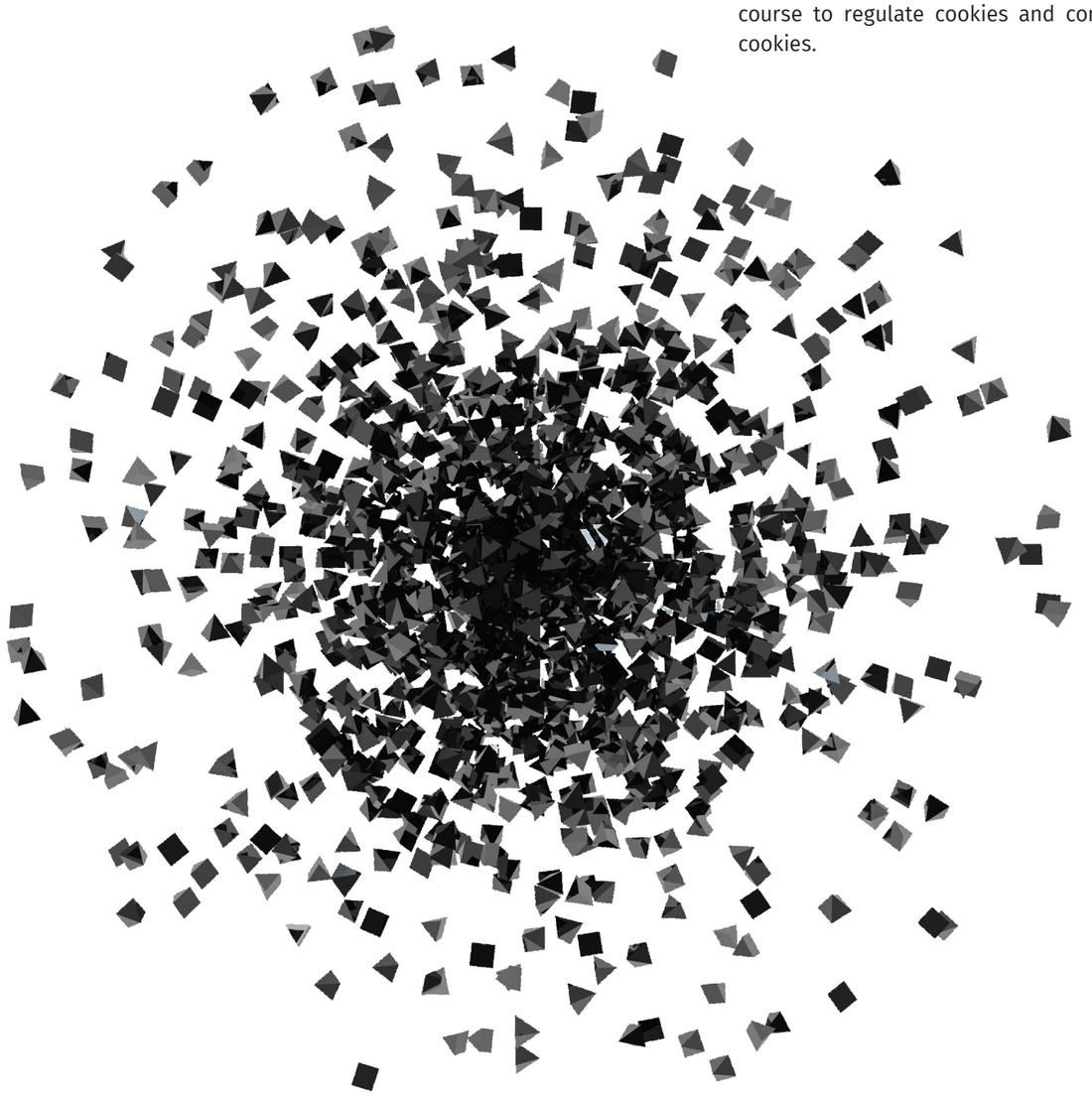
It is expected that the Board will:

- release a comprehensive list of countries with adequate level of protection;
- approve both undertakings between data controllers, and BCR.

B. Child Data Protection

The DP Law does not distinguish between personal data of adults and minors.

GDPR harmonizing amendments to the DP Law are expected to be introduced and to include specific provisions concerning protection of personal data of minors, including, but not limited to, procedures for obtaining explicit consent of minors.



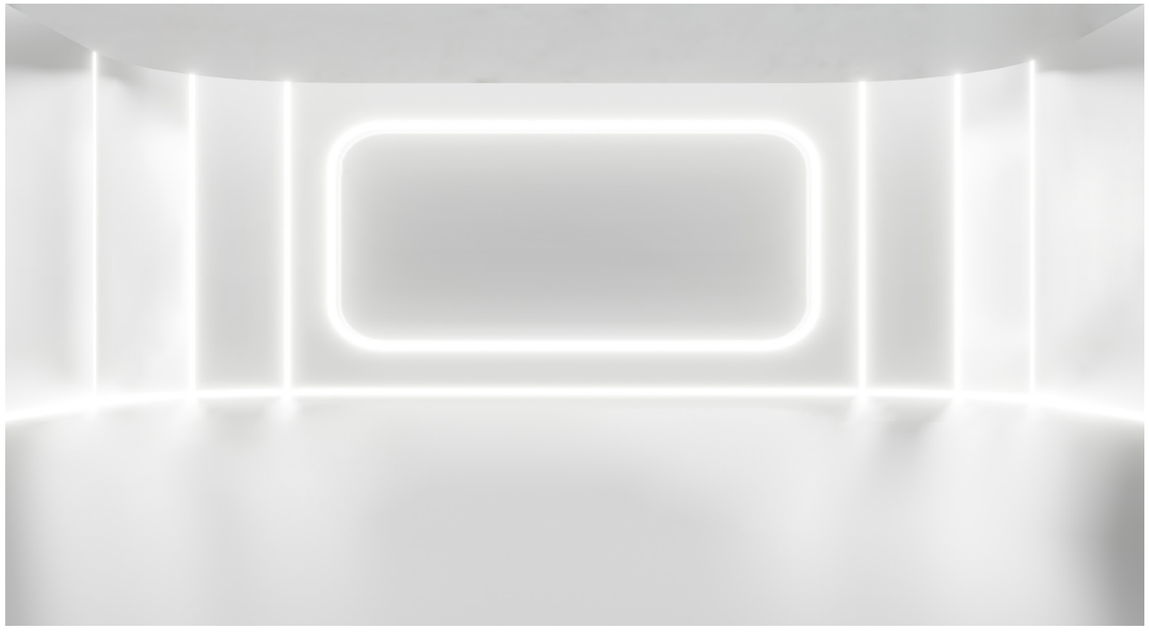
C. Cookies

The DP Law does not specifically address cookies, which, due to their nature, may be regarded as personal data if they can be used to identify a real person.

A regulation similar to the EU's e-Privacy Regulation is expected to be enacted in due course to regulate cookies and consent to cookies.

D. Data Localization

Turkish legislation provides certain data localization requirements for specific sectors, including banking and finance, payment systems, capital markets, telecommunications. Clarification of data localization rules and obligations is expected soon.



MOROĞLU ARSEVEN

Glossary

11th Development Plan	11th Development Plan of the Presidency of the Republic of Turkey for the years 2019 to 2023
Application Communiqué	Communiqué on Principles and Procedures for Application to Data Controller
Authority	Personal Data Protection Authority
BCR	Binding Corporate Rules
Board	Turkish Data Protection Board
Disclosure Communiqué	Communiqué on Procedures and Principles Regarding the Data Controller's Obligation to Inform
DP Law	Personal Data Protection Law No. 6698
EU	European Union
GDPR	General Data Protection Regulation
Health Regulation	Personal Health Data Regulation
KEP	Registered E-Mail
Ministry	Ministry of Health
Report	Activity Report for 2019 of Turkish Data Protection Board
VERBİS	Data Controller's Registry System

MOROĞLU ARSEVEN

Contacts

BURCU TUZCU ERSİN, LL.M.
Partner
btuzcu@morogluarseven.com
D: +90 (212) 377 47 50
T: +90 (212) 377 47 00

BURCU GÜRAY
Senior Associate
bguray@morogluarseven.com
D: +90 (212) 377 47 25
T: +90 (212) 377 47 00

CEYLAN NECİPOĞLU, PH.D, LL.M.
Senior Associate
cnecipoglu@morogluarseven.com
D: +90 (212) 377 47 35
T: +90 (212) 377 47 00

MOROĞLU ARSEVEN

www.morogluarseven.com

Abdi İpekçi Caddesi 19-1
Nişantaşı, İstanbul, 34367

T: +90 212 377 4700
F: +90 212 377 4799
info@morogluarseven.com