PANORAMIC

DATA PROTECTION & PRIVACY 2025

Contributing Editors

Aaron P Simpson and **Lisa J Sotto**

Hunton Andrews Kurth LLP

LEXOLOGY

Data Protection & Privacy 2025

Contributing Editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

Panoramic guide (formerly Getting the Deal Through) enabling side-by-side comparison of local insights into the legislative framework; relevant authorities; treatment of breaches; legitimate processing; data handling responsibilities of PII owners; security obligations; internal controls, including the data protection officer; registration formalities transfer and disclosure of PII; rights of individuals; judicial supervision; specific data processing use cases such as cookies, electronic communications marketing, and cloud services; and recent trends.

Generated on: July 9, 2024

Contents

Canada

Theo Ling, **Conrad Flaczyk**, **Matthew Cook**, **Nadia Rauf**
Baker McKenzie

Chile

Nicolás Yuraszeck, **Carlos Araya**, **Diego Lisoni**
Magliona Abogados

China

Gabriela Kennedy, **Joshua T K Woo**
Mayer Brown

France

Benjamin May, **Lou Mailhac**, **Anaël Boyer**
Aramis

Germany

Peter Huppertz
Hoffmann Liebs

Greece

Eugenia (Jenny) Georgountzou, **Natasha Mezini**, **Lambros Katsiamagkos**
GKP Law Firm

Hong Kong

Gabriela Kennedy, **Joshua T K Woo**
Mayer Brown

Hungary

Endre Várady, **János Tamás Varga**, **Andrea Belényi**
VJT & Partners

India

Stephen Mathias, **Arun Babu**
Kochhar & Co

Indonesia

Rusmaini Lenggogeni, **Charvia Tjhai**
SSEK Law Firm

Ireland

Shane Martin, **Conor Daly**, **Coleen Wegmann**, **Susan Battye**
Walkers

Italy

Paolo Balboni, **Luca Bolognini**, **Antonio Landi**, **Davide Baldini**
ICT Legal Consulting

Japan

Masaki Mizukoshi, **Saaya Shiina**
Nagashima Ohno & Tsunematsu

Kazakhstan

Saule Akhmetova
GRATA International

Malaysia

Jillian Chia Yan Ping, **Natalie Lim**, **Beatrice Yew**
SKRINE

Malta

Paul Gonzi, **Antonio Ghio**
Fenech & Fenech Advocates

New Zealand

Derek Roth-Biester, **Megan Pearce**, **Nick Tinholt**
Anderson Lloyd

Pakistan

Saifullah Khan, **Saeed Hasan Khan**
S.U.Khan Associates Corporate & Legal Consultants

Poland

Marcin Lewoszewski, **Anna Kobylańska**, **Arwid Mednis**
Kobylanska Lewoszewski Mednis

Portugal

Helena Tapp Barroso, **Tiago Félix da Costa**
Morais Leitão, Galvão Teles, Soares da Silva & Associados

Serbia

Bogdan Ivanišević, **Anja Gligorević**
BDK Advokati

Singapore

Lim Chong Kin, **Anastasia Su-Anne Chen**
Drew & Napier LLC

South Korea

Kwang Hyun Ryoo, **Tae Uk Kang**, **Minwoon Yang**, **Minyoung Kim**
Bae, Kim & Lee LLC

Switzerland

Lukas Morscher, **Leo Rusterholz**
Lenz & Staehelin

Taiwan

Yulan Kuo, **Jane Wang**, **Brian Hsiang-Yang Hsieh**, **Emily Hsu**
Formosa Transnational Attorneys at Law

Thailand

John Formichella, **Naytiwut Jamallsawat**, **Onnicha Khongthon**, **Supitchaya Akeyati**
Formichella & Sritawat Attorneys at Law

Türkiye

Esin Çamlıbel, **Beste Yıldızili Ergül**, **Naz Esen**, **Canberk Taze**
Turunç

United Arab Emirates

Saifullah Khan, **Saeed Hasan Khan**
Bizilance Legal Consultants

United Kingdom

Aaron P Simpson, **Sarah Pearce**, **James Henderson**, **Jonathan Wright**
Hunton Andrews Kurth LLP

USA

Aaron P Simpson, **Danielle Dobrusin**
Hunton Andrews Kurth LLP

Türkiye

Esin Çamlıbel, Beste Yıldızili Ergül, Naz Esen, Canberk Taze
Turunç

Summary

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The Turkish Constitution has specifically protected personal information (PI) since 2010.

Protection of PI is regulated by specific legislation, namely the Personal Data Protection Law (PDPL), Law No. 6698, which came into force in October 2016. Directive 95/46/EC is the starting point for the PDPL. Even though there are various differences between the PDPL and the General Data Protection Regulation (GDPR), the PDPL is generally based on and follows the GDPR.

The Turkish Parliament recently adopted significant amendments to the PDPL. These amendments became effective on 1 June 2024 and are described throughout this chapter.

Turkey is party to the Convention for the Protection of Individuals with regard to Automated Processing of Personal Data of 1981 of the Council of Europe (Convention 108). The Convention was published in the Turkish Official Gazette in March 2016 and became domestic law.

Crimes against data protection and related sanctions are also regulated by the Turkish Criminal Code.

Law stated - 1 June 2024

Data protection authority

2 Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The authority responsible for overseeing the implementation of the PDPL is the Personal Data Protection Authority (the Authority). The Authority is responsible, among other things, for monitoring the latest developments in legislation and practice, making evaluations and recommendations, conducting research and analyses, and cooperating with public institutions and organisations, international organisations, non-governmental organisations, professional associations and universities.

The Data Protection Board (Board) is formed within the Authority and has the following duties, among others:

- ensuring that personal data are processed in compliance with the PDPL, and fundamental rights and freedoms;
- promulgating rules and regulations under the PDPL;
- determining administrative sanctions under the PDPL;

- reviewing complaints of PDPL violations;
- taking necessary measures against PDPL violations at its own discretion;
- setting a strategic plan for the Authority;
- determining the purpose, targets, service quality standards and performance criteria of the Authority;
- determining additional measures for the processing of sensitive personal data;
- determining specific rules regarding data security, and the duties, powers and responsibilities of data controllers;
- providing comments on legislation and rules drafted by other institutions and organisations that include personal data provisions; and
- approving and publishing periodic reports on the performance, financial situation, annual activities and other matters related to the Authority.

Law stated - 1 June 2024

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The Authority is the sole authorised institution under the PDPL. The PDPL tasks the Authority with monitoring and evaluating international developments on personal data issues, and cooperating with international organisations and foreign counterparts.

Despite the limited number of decisions the Board has issued since its formation, the visible trend is that the Board takes decisions of the European Data Protection Board into account when investigating cases. However, there is no mechanism to prevent the Board from taking decisions diverging from those of the European Data Protection Board.

Law stated - 1 June 2024

Breaches of data protection law

4 Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Breach of the PDPL can lead to both administrative fines and criminal penalties. The Board is responsible for ensuring that personal data is processed in compliance with fundamental rights and freedoms, and reviewing complaints of data subjects. The Board can take temporary measures and other adequate measures, such as monetary sanctions, against violations.

In addition, criminal acts such as the unlawful acquisition or registration of personal data, and non-destruction of personal data when required may be subject to criminal penalties under the Turkish Criminal Code.

Law stated - 1 June 2024

Judicial review of data protection authority orders

5 | Can PI owners appeal to the courts against orders of the data protection authority?

As of 1 June 2024, lawsuits against the orders of the Authority are filed only in administrative courts, within 60 days of the delivery of the relevant order.

Previously, data subjects could appeal to criminal courts of peace against the orders of the Authority. Such applications pending as of 1 June 2024 before the criminal courts of peace against the orders of the Authority will continue to be decided by criminal courts of peace.

Law stated - 1 June 2024

SCOPE

Exempt sectors and institutions

6 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

PDPL applies to all natural persons whose personal data are processed. It also applies to all natural and legal persons who process such data using fully or partially automated means or, provided that they are part of a data registry system ('filing system' under the GDPR), through non-automated means. There is no distinction foreseen between private sector institutions and state institutions. As such, the PDPL is applicable to all types of entities and persons.

However, the PDPL does not apply in the following cases:

- processing by natural persons within the scope of activities relating to either themselves or their family members living in the same household, on the condition that the data is safeguarded and not provided to third parties;
- anonymised processing for statistical, research, planning and similar purposes;
- processing for the purposes of art, history, literature and science, or as part of the exercise of freedom of speech, provided the processing does not prejudice national defence, national security, public order, public safety, economic security, privacy and other personal rights, or constitute a crime;
- processing within the scope of preventive, protective and intelligence activities by state institutions carrying out national defence, national security, public order, public safety or economic security functions; and
- processing by judicial authorities or execution authorities in relation to investigations, prosecutions, court cases, criminal proceedings, and execution and enforcement proceedings.

Law stated - 1 June 2024

Interception of communications and surveillance laws

7 Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

No, the PDPL does not directly cover interception of communications, electronic marketing or monitoring and surveillance of individuals. Having said that, the Board has issued a decision regarding the regulation of contacting individuals via email, SMS or phone calls to make advertisements, where it held that such communications are subject to the same principles under the PDPL as it applies to other data processing. Accordingly, these types of communications can be made only based on consent or in reliance on an exemption.

Turkey has specific legislation that covers the interception of communications, electronic marketing, and monitoring and surveillance of individuals. For example, the Law on Electronic Communication regulates all electronic communication methods, while the Law on Electronic Trade regulates electronic marketing and trade. The Regulation on Erasure, Destruction and Anonymisation of Personal Data and the Communiqué on Rules and Procedures for the Fulfilment of the Obligation to Inform determine the rules and procedures to be applied to interception of communications, electronic marketing, and monitoring and surveillance of individuals. The Board has also published guidance regarding electronic communications bearing personal information and deemed it necessary for data controllers to take reasonable measures to verify the contact information declared by the relevant data subjects (eg, sending a verification code or link to the person's registered phone number or email address). Per the Board's approach, keeping personal data accurate and up-to-date is both in the interest of the data controller and necessary to protect the fundamental rights and freedoms of the data subject. In addition, channels must be made available at all times for data subjects to update their personal data. The Criminal Code and Criminal Procedural Law regulate the sanctions in case of breach of applicable legislation.

Law stated - 1 June 2024

Other laws

8 Are there any further laws or regulations that provide specific data protection rules for related areas?

There are specific rules setting forth data protection rules for various areas. As an example, Turkish Labour Law holds that employers are obliged to use the personal data of employees in good faith and in accordance with applicable law, and not to disclose any personal data in which an employee has legitimate interest and has requested to be kept private.

Another example is the Regulation on Processing and Maintaining Privacy of Personal Health Data, regulating the rules and procedures to be used while processing data involving health information.

Turkish Banking Law, the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions and the Law on Bank Cards and Credit Cards regulate the processing and transfer of financial data in Turkey and abroad.

Turkish telecommunications legislation also has provisions regarding data processing and transfers.

Law stated - 1 June 2024

PI formats

9 | What categories and types of PI are covered by the law?

The PDPL does not limit the scope of protection by categories or types. All information relating to an identified or identifiable natural person maintained and stored in any format is covered by the PDPL and secondary legislation promulgated thereunder. However, there are specific provisions in the PDPL that regulate sensitive personal data as 'special categories of personal data'.

Law stated - 1 June 2024

Extraterritoriality

10 | Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The PDPL does not make any differentiation between data subjects who are nationals or not. The PDPL is applicable to all natural persons whose personal data are processed.

With recent amendments to the PDPL, which came into effect on 1 June 2024, there are three permitted categories for transfer of personal data abroad, as described in detail below. Prior to the amendments, the general explicit consent route was also available for data transfers abroad. While this route has been eliminated, previously obtained consents will continue to be valid until 1 September 2024.

Data transfer to countries where there is adequate protection

Personal data may be transferred abroad by data controllers and data processors if one of the conditions specified in the PDPL for processing of personal data or sensitive personal data is met and there is an adequate protection decision by the Board regarding the relevant country, sectors within the country or international organisations. The Board will weigh different factors, including the principle of reciprocity, when making an adequate protection decision.

With the amendments, it has been made possible for the Board to decide on adequacy for specific sectors of a country and international organisations, as well as countries as a

whole. That said, although the authority to declare countries with adequate protection has been available since 2016, no country has yet been designated as such.

Taking adequate measures (appropriate safeguards)

If there is no adequacy decision per above, the transfer of personal data abroad will be possible if one of the conditions specified in the PDPL for processing of personal data or sensitive personal data is met and the data subject has the right to exercise its rights and apply to legal remedies in the relevant country, and if one of the following conditions applies:

- if an agreement (that is not qualified as an international treaty) is signed between foreign public institutions or organisations, or international organisations on the one hand, and public institutions or professional organisations qualified as public institutions in Turkey on the other hand, and the transfer is approved by the Board,
- for multinational companies, where binding corporate rules with which all the undertakings are obliged to comply have been approved by the Board,
- if the standard contract published by the Board and containing the purposes of the personal data transfer, the transferred data categories, transferees and transferee groups, the technical and administrative measures to be taken by the transferee, and additional measures for sensitive personal data, is used; or
- if the data controllers in Turkey and in the relevant foreign country undertake to provide adequate protection in writing and the transfer is approved by the Board.

For all of the options described above, in addition to the requirement that one of the conditions specified in the PDPL for processing of personal data or sensitive personal data is met, it is also necessary for the data subject to have the right to be able to exercise their rights and apply to legal remedies in the jurisdiction to which the personal data will be transferred. The Authority has not yet announced which countries provide data subjects the right to exercise their rights and apply for legal remedies.

It is important to note that if a standard contract is used for transfers abroad, the contract must be reported to the Authority by the data controller or the data processor within five business days following the signing. If the contract is not reported to the Authority, administrative fines ranging from 50,000 to 1 million lira may be imposed on those who do not fulfil their obligation to notify.

Furthermore, the data processor as well as the data controller is considered to be responsible for transfers abroad, and accordingly, administrative fines may be levied on data processors who do not fulfil their obligation to notify the Authority.

Temporary transfers abroad

In cases where neither the adequacy grounds nor the appropriate safeguards route described above are met, provided that it is non-repetitive (transfer of once or few times in a non-permanent manner), transfer of personal data abroad will be possible if:

- explicit consent of the data subject is obtained, provided they have been informed about the potential risks;
- the transfer is necessary for the performance of a contract between the data subject and the data controller, or to perform the precautions requested by the data subject before the contract was executed;
- the transfer is necessary for the establishment or performance of a contract for the benefit of the data subject that is signed between the data controller and another natural or legal person;
- the transfer is necessary for a superior public benefit;
- the transfer is necessary for the establishment, exercise or protection of a right;
- processing data is necessary for the protection of the life or body integrity of persons who cannot express their consent due to physical impossibility or whose consent is not legally valid; or
- the transfer is made from a registry open to the public or to persons with legitimate interests, provided that the necessary conditions set by the relevant legislation to access the registry are met and transfer is requested by a person with legitimate interest.

Data controllers and data subjects must first transfer personal data abroad in line with the general rules. If this is not possible, the transfer may be made temporarily (ie, non-repetitively) in line with the above rules. In this context, transfer to a company located abroad is possible to carry out commercial activities, provided that this transfer will be made once or a few times, and not permanently. Accordingly, the temporary transfer route should not be interpreted as allowing data controllers to use servers located abroad on a permanent basis.

Regardless of the method used to transfer personal data abroad, data controllers and data processors are obligated to take the appropriate safeguards set forth in the PDPL, and ensure that the conditions for transfer abroad are applied for ongoing transfers after the initial transfer of personal data abroad.

Additionally, data controllers and data processors need to have familiarity with the transferee country and its laws, and to monitor the transfer at every stage.

Nevertheless, the implementation procedures for data transfers abroad have yet to be determined by regulations. In early May 2024, the Authority published the Draft Regulation on the Procedures and Principles Regarding the Transfer of Personal Data Abroad. The Draft Regulation mainly repeats the transfer routes laid out by the PDPL through the recent amendments thereto, and regulates the use and signature process of standard contracts for transfer. The Authority is currently seeking comments on the public Draft Regulation, and is expected to publish the final version soon.

Hence, the applicability of the PDPL is not limited to Turkey.

Law stated - 1 June 2024

Covered uses of PI

11 Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The PDPL covers all processing and use of personal data. Certain distinctions are made among the owners, controllers and processors with respect to their duties and liabilities.

Law stated - 1 June 2024

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

12 Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

As a general rule, personal data cannot be processed without the explicit consent of the data subject. However, if one of the following conditions is met, personal data may be processed without seeking the explicit consent of the data subject:

- the processing is clearly provided for by applicable law;
- the processing is necessary to protect the life or bodily integrity of a person who is unable to give consent due to actual impossibility or whose consent is not legally recognised, or the life or bodily integrity of another person;
- the processing is necessary for the formation or performance of a legal contract to which the data subject is party to;
- the processing is necessary to comply with a legal obligation to which the data controller is subject;
- the data has been made public by the data subject;
- the processing is necessary to establish, use or protect a legal right; and
- the processing is necessary for the purposes of legitimate interests pursued by the controller, provided that the fundamental rights and freedoms of the data subject are not harmed.

Pursuant to the Board's decisions, data processors can request the explicit consent of the data owners only if the above circumstances are not present.

Law stated - 1 June 2024

Legitimate processing – types of PI

13 Does the law impose more stringent rules for processing specific categories and types of PI?

Under article 6 of the PDPL, personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, clothing choices and habits, trade union membership, health or sex life, criminal conviction and security measures, and biometric or genetic information are defined as sensitive personal data. As a general rule, these categories of data may be processed, as of 1 June 2024, only in the following circumstances:

- where the data subject has given explicit consent for the processing of sensitive personal data;
- processing of sensitive personal data, including health and sexual life data, is permitted by applicable law;
- processing of sensitive personal data is necessary to protect the life or body integrity of persons who cannot express their consent due to physical impossibility or whose consent is not legally valid;
- processing of sensitive personal data relates to data made public by the data subject and the processing is consistent with the subject's intention to make the data public;
- processing of sensitive personal data is necessary for the establishment, exercise or protection of a right;
- processing of sensitive personal data by persons who are under the obligation of confidentiality, or by authorised institutions and organisations is necessary for the protection of public health, preventative medicine, medical diagnosis, the delivery of treatment and care, and the planning, management and finance of healthcare services;
- processing of sensitive personal data is compulsory to fulfil legal obligations regarding employment, occupational health and safety, social security, social services, or social aid; and
- processing of sensitive personal data is undertaken by foundations, associations and other non-profit organisations or entities established for political, philosophical, religious or union purposes with respect to their current or former members, or persons who are in regular contact with these organisations and entities, where the processing complies with applicable law and their purposes, is limited to their fields of activity and is not disclosed to third parties.

Processing of data must be in compliance with the purposes stated in the data processing notification. If the processor decides to process the data for any reason other than those stated in the data processing notification, a new notification stating the new purpose must be provided to the data subject.

The Board has issued heightened measures for the safekeeping and processing of sensitive personal data. These measures include, among others, training programs, encryption requirements, two-factor authentication for remote access and physical security measures such as access controls.

Law stated - 1 June 2024

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

14 Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

When processing personal data, the controller or the person authorised by the controller is obliged to inform the data subjects. The notification must include:

- the identity of the controller and of its representative, if any;
- the purpose of the data processing;
- to whom and for what purposes the processed data may be transferred;
- the method and legal basis for the collection of the personal data; and
- the rights of the data subjects accorded by the PDPL.

The notification must be provided at the time of the acquisition of the data, and must use easy-to-understand, clear and plain language. If the personal data are obtained from a third party (ie, not the data subject), the notification must be made within a reasonable time after the data are obtained, at the time of first contact if obtained for the purpose of communication, and at the time of first transfer if obtained for the purpose of transferring.

Law stated - 1 June 2024

Exemptions from transparency obligations

15 When is notice not required?

A notice is not required if:

- processing of the personal data is necessary to prevent a crime or for a criminal investigation;
- the data subject has him or herself made the personal data public;
- processing of the personal data is required for supervisory, regulatory or disciplinary activities to be carried out by public institutions and professional associations with public institution status; or
- processing of the personal data is required for protection of the state's economic and financial interests with regard to budgetary, tax-related and financial issues.

Law stated - 1 June 2024

Data accuracy

16 Does the law impose standards in relation to the quality, currency and accuracy of PI?

Personal data must be:

- processed lawfully and fairly;
- accurate and, where necessary, kept up to date;
- collected for specified, explicit and legitimate purposes;
- relevant and limited to the purposes for which they are processed; and
- retained only for the period stipulated by relevant legislation or the purpose for which they are processed.

Law stated - 1 June 2024

Data minimisation

17 | Does the law restrict the types or volume of PI that may be collected?

According to the PDPL, the amount of data processed must be proportionate to the purpose of the processing, and the amount must be as small as possible. Any data processing that exceeds the purpose of processing will be unlawful. Data controllers must avoid processing data that is disproportionate to achieving the purpose of processing (eg, to avoid processing sensitive personal data for entry into work, when the same purpose could be achieved without processing any or minimal personal data).

Law stated - 1 June 2024

Data retention

18 | Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

There is no restriction on the amount of personal data that may be held. However, personal data can be preserved only for the periods foreseen in the applicable regulations or the periods necessary for the purpose of the processing.

In addition, the amount of data and the length of time the data may be held for must be proportionate to the purpose of the processing, and both the amount and length must be as small as possible.

While determining the maximum storage period, the following must be taken into account:

- generally accepted storage periods in the sector in which the data controller operates;
- the length of time for which the legal relationship with the data subject that is the basis of the processing will continue;
- the length of time for which the legitimate interest of the data controller in accordance with lawfulness and fairness principles will continue;

- the length of time during which the risks, costs and responsibilities arising from the storage of the relevant data category will legally continue;
- whether the intended maximum storage period is suitable to keep the relevant data category accurate and up to date;
- the length of time during which the data controller is obliged to store the data pursuant to its legal obligations; and
- the period of limitation determined by the data controller for the assertion of a right relating to personal data in the relevant data category.

Those data controllers who are obliged to register with the Data Controllers Registry, known as VERBİS (Veri Sorumluları *Sicil Bilgi Sistemi), are also obliged to prepare a data inventory, as well as data preservation and destruction policies, which set forth, among other things, the periods during which personal data will be preserved.*

Data controllers who are required to prepare data preservation and destruction policies must erase, destroy or anonymise, as applicable, the relevant data at regular intervals upon the triggering of such obligation. These periods cannot exceed six months. On the other hand, for data controllers who are not required to prepare data preservation and destruction policies, this period cannot exceed three months.

Records of all erasure, destruction and anonymisation activities must be kept and stored for at least three years (subject to any other applicable legal obligations).

Law stated - 1 June 2024

Purpose limitation

19 Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Yes, the purposes for using the personal data must be determined and the data subject accordingly informed when obtaining the consent of the data subject. Data controllers cannot exceed or circumvent these purposes. Furthermore, regardless of whether the processing of personal information is based on the consent of the data owner or a legitimate ground not requiring consent, the processing purposes must be disclosed to the data subjects. An organisation must inform the data subjects or, where applicable, obtain explicit consent from the data subjects to exceed the purposes for which the data was initially collected.

Law stated - 1 June 2024

Automated decision-making

20 Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

There is no prohibition on using automated decision systems or making automated decisions without human intervention. The general principles of the PDPL, such as informing the data subject, shall always apply.

Additionally, as per the PDPL, data subjects can always object to the results of automated decision-making.

Law stated - 1 June 2024

SECURITY

Security obligations

21 What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Data controllers are obliged to take all necessary technical and administrative measures to provide a sufficient level of security. Data controllers must also conduct necessary inspections or have them conducted in their own institutions. While there are no specific standards established for the technical and administrative measures to be used, the relevant guidelines of the Data Protection Board (the Board) set forth various possible data security measures. These measures include, among other things, establishing a data matrix, using closed-circuit systems, using firewalls and antivirus programs, and implementing data security policies.

Law stated - 1 June 2024

Notification of data breach

22 Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Under the Personal Data Protection Law, in cases where the processed data is obtained by third parties through unlawful methods, the controller must notify the data subject and the Board as promptly as possible and, in any event, within 72 hours. Where necessary, the Board may announce such breach on its official website or through other methods it deems appropriate.

Law stated - 1 June 2024

INTERNAL CONTROLS

Accountability

23 Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Under the PDPL, data controllers are under an obligation to implement all necessary technical and administrative precautions to maintain data security. While the legislation does not specifically include an obligation to maintain internal controls, data controllers who are obliged to register with the Data Controllers Registry are also obliged to prepare data preservation and destruction policies, which must contain, among other things, extensive information on how the data will be processed internally. The Board also recommends signing confidentiality agreements with the employees for data breach cases.

Furthermore, if an international company adopts binding corporate rules, and these rules are approved by the Board to transfer personal data abroad without the explicit consent of the data subject, the company and its group companies will be required to set up an internal compliance mechanism in accordance with the law.

Law stated - 1 June 2024

Data protection officer

24 Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The PDPL does not foresee an obligation for appointing a data protection officer. However, in 2021, the Board published the Communiqué on Procedures and Principles of Personnel Certification Mechanism (Communiqué) and the Programme on Certification of Data Protection Personnel (Programme). The Communiqué and the Programme explain the certification process of data protection personnel in terms of competence and procedural requirements for accreditation. For example, data protection personnel must pass a written exam and meet the minimum requirements determined by the Board to obtain their certificates. Although the obligations of data protection personnel have not yet been set, the Board is laying the legal groundwork to implement a similar function to that of a data protection officer in the near future.

Law stated - 1 June 2024

Record-keeping

25 Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

The PDPL does not contain a provision regarding a general obligation to maintain internal records. Having said that, data controllers and processors who process personal data by automated means are obliged to register with the Data Controllers Registry (VERB0S) and establish a personal data processing inventory, which must include the purpose and the legal reason for the processing, the data category, to whom the data will be transferred, the period of preservation, data to be transferred abroad, and the precautions taken for data security.

Those data controllers who are obliged to register with the Data Controllers Registry are also obliged to prepare data preservation and destruction policies, which set forth, among other things, the periods during which personal data will be preserved.

In addition to the PDPL, the Law on Electronic Communications and related regulations oblige licensed operators within the electronic communications sector to maintain certain records relating to electronic communications. Licensed operators are also under an obligation to keep access records of personal data for two years.

Law stated - 1 June 2024

Risk assessment

26 Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Data controllers are at all times obliged to take all necessary technical and administrative measures to provide a sufficient level of security. However, the Board particularly focuses on whether the personal data is sensitive, as well as the confidentiality level of the data and the possible damages to the data subject in the event of a security breach. While there are no specific standards established for the technical and administrative measures to be used, the relevant guidelines of the Board set forth various possible data security measures. These measures include, among other things, informing employees regarding possible security breaches, establishing a data matrix, using closed-circuit systems, using firewalls and antivirus programs, and implementing data security policies.

Law stated - 1 June 2024

Design of PI processing systems

27 Are there any obligations in relation to how PI processing systems must be designed?

The Board has issued heightened measures for the safekeeping and processing of sensitive personal data. However, there are no specific obligations as such in relation to personal information processing systems outside of sensitive personal data.

Law stated - 1 June 2024

REGISTRATION AND NOTIFICATION

Registration

28 Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

As a general rule, data controllers are required to register with VERB0S. The Board has exempted, through various decisions, the following data controllers from the registration requirement:

- data processors who are part of a data registry system ('filing system' under the GDPR) and process data only in non-automated ways;
- associations, foundations and unions resident in Turkey, to the extent they process data in compliance with relevant legislation and their purposes, and in any case limited to their areas of activity;
- political parties;
- lawyers;
- mediators;
- notaries public;
- certified public accountants;
- customs brokers; and
- employers who employ fewer than 51 people and whose annual net assets do not exceed 100 million lira, provided their primary line of business is not the processing of sensitive personal data.

Data controllers who are not exempt from the obligation to register must register with VERB0S at verbis.kvkk.gov.tr. As part of the registration process, data controllers must appoint a contact person and complete the form provided by the Authority. If the data controller is in a foreign country, a data controller representative resident in Turkey must be appointed.

The following information must be registered with VERB0S by the data controller:

- the identity and address of the data controller and of its representative (if any);
- the purpose for which the personal data will be processed;
- explanations relating to groups of data subjects and the relevant data categories of the subjects;
- the recipients or groups of recipients to whom the personal data may be transferred;
- the personal data envisaged to be transferred abroad;
- the measures taken concerning the security of the personal data; and
- the maximum storage period necessary for the purpose for which the personal data are processed.

Registration and renewals are not subject to any fees.

See https://www.kvkk.gov.tr/Icerik/6635/By-Law-On-Data-Controllers-Registry.

Persons who fail to comply with the obligation to register with and maintain proper entries on VERB0S may be sanctioned with a monetary fine between 189,245 lira and 9,463,213 lira by the Board.

Law stated - 1 June 2024

Other transparency duties

29 | Are there any other public transparency duties?

Public companies have a general duty to disclose information on events that may affect their investors' decisions. While this requirement is not specifically regulated for data processing, matters relating to data privacy will need to be disclosed if sufficiently material. There are no other transparency duties; data processors are only obliged to notify the data subjects as required by the PDPL and register with VERB0S when the applicable conditions are met.

Law stated - 1 June 2024

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

30 | How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The Personal Data Protection Law (PDPL) foresees special conditions for the domestic transfer of personal data. Personal data normally cannot be transferred without a legitimate ground specified in the PDPL or the explicit consent of the data subject. Hence, the data controller must notify the data subject that personal data will be transferred to third parties providing outsourced processing services, and obtain the data subject's consent in the event that the transfer is not based on a legitimate ground (such as advertisement purposes). In the event that the data subject denies providing consent and the processing is not based on a legitimate ground, the applicable personal data must be destroyed (or, if applicable consent or grounds exist, used by the data processor without the involvement of the outsourced service). Furthermore, for personal data required to be preserved pursuant to various legislations, data owners are required to establish a system for preserving such personal data without transferring it to third parties.

The PDPL also requires that data owners who use outsourced processing services provide sufficient protection with regard to the processing and preservation of personal data. In the event of a breach, data owners are jointly and severally liable with the entities providing outsourced processing services for the compensation of any damages.

Law stated - 1 June 2024

Restrictions on third-party disclosure

31 | Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

As a general rule, there are no specific restrictions foreseen on the sharing of personal data apart from the general requirements detailed above as to notifying and informing the data subject, obtaining the data subject's consent (except the conditions specified in the PDPL pursuant to which personal data can be transferred within Turkey without obtaining explicit consent) as to what data will be disclosed, and determining the purposes for which the data shall be disclosed.

Having said that, for sharing sensitive personal data, the Board has set forth additional precautions and restrictions. These include the transfer of data in an encrypted format and for hard copies of the data to be labelled as classified. In addition, it is mandatory to obtain the data owner's consent unless the processing is required by law. In its guidelines, the Board specifically refers to the selling of sensitive personal data as a data breach, and Turkish Criminal Law states that the person who gives, distributes or seizes personal data unlawfully is punished with imprisonment from two to four years.

Law stated - 1 June 2024

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

With the recent amendments to the PDPL, which came into effect on 1 June 2024, there are three permitted categories for the transfer of personal data abroad, as described in detail below. Prior to the amendments, the general explicit consent route was also available for data transfers abroad. While this route has been eliminated, previously obtained consents will continue to be valid until 1 September 2024.

Data transfer to countries where there is adequate protection

Personal data may be transferred abroad by data controllers and data processors if one of the conditions specified in the PDPL for processing of personal data or sensitive personal data is met and there is an adequate protection decision by the Board regarding the relevant country, sectors within the country or international organisations. The Board will weigh different factors, including the principle of reciprocity, when making an adequate protection decision.

With the amendments, it has been made possible for the Board to decide on adequacy for specific sectors of a country and international organisations, as well as countries as a whole. That said, although the authority to declare countries with adequate protection has been available since 2016, no country has yet been designated as such.

Taking adequate measures (appropriate safeguards)

If there is no adequacy decision per above, the transfer of personal data abroad will be possible if one of the conditions specified in the PDPL for processing of personal data or sensitive personal data is met and the data subject has the right to exercise its rights

and apply to legal remedies in the relevant country, and if one of the following conditions applies:

- if an agreement (that is not qualified as an international treaty) is signed between foreign public institutions or organisations, or international organisations on the one hand, and public institutions or professional organisations qualified as public institutions in Turkey on the other hand, and the transfer is approved by the Board;
- for multinational companies, where binding corporate rules with which all the undertakings are obliged to comply have been approved by the Board;
- if the standard contract published by the Board and containing the purposes of the personal data transfer, the transferred data categories, transferees and transferee groups, the technical and administrative measures to be taken by the transferee, and additional measures for sensitive personal data, is used; or
- if the data controllers in Turkey and in the relevant foreign country undertake to provide adequate protection in writing and the transfer is approved by the Board.

For all of the options described above, in addition to the requirement that one of the conditions specified in the PDPL for processing of personal data or sensitive personal data is met, it is also necessary for the data subject to have the right to be able to exercise their rights and apply for legal remedies in the jurisdiction to which the personal data will be transferred. The Authority has not yet announced which countries provide data subjects the right to exercise their rights and apply for legal remedies.

It is important to note that if a standard contract is used for transfers abroad, the contract must be reported to the Authority by the data controller or the data processor within five business days following the signing. If the contract is not reported to the Authority, administrative fines ranging from 50,000 to 1 million lira may be imposed on those who do not fulfil their obligation to notify. Another important aspect of the relevant amendment is that the data processor as well as the data controller is considered to be responsible for the transfer abroad, and accordingly, administrative fines are determined for data processors who do not fulfil their obligation to notify the Authority.

Temporary transfers abroad

In cases where neither the adequacy grounds nor the appropriate safeguards route described above are met, provided that it is non-repetitive (transfer of once or a few times in a non-permanent manner), transfer of personal data abroad will be possible if:

- explicit consent of the data subject is obtained, provided they have been informed about the potential risks;
- the transfer is necessary for the performance of a contract between the data subject and the data controller, or to perform the precautions requested by the data subject before the contract was executed;
- the transfer is necessary for the establishment or performance of a contract for the benefit of the data subject that is signed between the data controller and another natural or legal person;

- the transfer is necessary for a superior public benefit;
- the transfer is necessary for the establishment, exercise or protection of a right;
- processing data is necessary for the protection of the life or body integrity of persons who cannot express their consent due to physical impossibility or whose consent is not legally valid; or
- the transfer is made from a registry open to the public or to persons with legitimate interests, provided that the necessary conditions set by the relevant legislation to access the registry are met and transfer is requested by a person with legitimate interest.

Data controllers and data subjects must first transfer personal data abroad in line with the general rules. If this is not possible, the transfer may be made temporarily (ie, non-repetitively) in line with the above rules. In this context, transfer to a company located abroad is possible to carry out commercial activities, provided that this transfer will be made once or a few times, and not permanently. Accordingly, the temporary transfer route should not be interpreted as allowing data controllers to use servers located abroad on a permanent basis.

All this said, the implementation procedures of data transfers abroad have yet to be determined by regulations. In early May 2024, the Authority published the Draft Regulation on the Procedures and Principles Regarding the Transfer of Personal Data Abroad. The Draft Regulation mainly repeats the transfer routes laid out by the PDPL through the recent amendments thereto, and regulates the use and signature process of standard contracts for transfer. The Authority is currently seeking comments on the public Draft Regulation, and is expected to publish the final version soon.

Law stated - 1 June 2024

Further transfer

33 If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Yes, if transfers outside of Turkey are subject to restriction or authorisation, these will also apply to transfers to service providers and onward transfers.

Regardless of the method used to transfer personal data abroad, data controllers and data processors are obligated to take the appropriate safeguards set forth in the PDPL, and ensure that the conditions for transfer abroad are applied for ongoing transfers after the initial transfer of personal data abroad.

Additionally, data controllers and data processors need to have familiarity with the transferee country and its laws, and to monitor the transfer at every stage.

Law stated - 1 June 2024

Localisation

34 Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

The PDPL does not require the personal information (PI) or copy of PI to be retained in Turkey. However, certain regulatory bodies, such as the Capital Markets Board of Turkey and the Central Bank of the Republic of Turkey, often require companies subject to their enforcement to have their own information systems, and therefore keep PI in Turkey.

Law stated - 1 June 2024

RIGHTS OF INDIVIDUALS

Access

35 Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Under the Personal Data Protection Law (PDPL), everyone has the right to:

- learn whether or not his or her personal data has been or is being processed;
- request information as to the processing if his or her data has been processed;
- learn the purpose of the processing and whether data is used in accordance with such purpose; and
- know the identity of the third parties in Turkey and abroad to whom personal data has been transferred.

Data subjects can use these by directly applying to the data controller in writing (in Turkish). Data controllers are obliged to respond to requests within 30 days. There are no limitations or fees associated with exercising these rights, except that the data controller may pass on any costs it incurs (eg, the cost of a flash drive sent to the data subject).

Law stated - 1 June 2024

Other rights

36 Do individuals have other substantive rights?

Each data subject has the right to apply to the controller and:

- request the rectification of any incomplete or inaccurate data;
- request the erasure or destruction of his or her personal data (subject to the conditions specified in the PDPL);
- request notification of the actions listed in the first two bullet points above to third parties to whom his or her personal data have been transferred;
-

object to any unfavourable result or consequence for the data subject, if such result or consequence is the result of exclusively automated means of the processing of his or her personal data; and

- request compensation and other remedies for damages arising from any unlawful processing of his or her personal data.

Law stated - 1 June 2024

Compensation

37 Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Yes. Despite the fact that the PDPL does not foresee any compensation for data subjects who are affected by breaches of the PDPL, individuals can resort to general provisions of law and claim material and moral damages foreseen by the Turkish Code of Obligations. To claim material damages, the data subject must prove that damage has occurred due to the fault of the data controller. On the other hand, to claim moral damages, the data subject must demonstrate that there was a violation of his or her individual rights and freedoms, and that violation has caused grave psychological harm.

Law stated - 1 June 2024

Enforcement

38 Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Data subjects may demand that their rights in the PDPL, such as the right to be informed whether their PII is being processed, the purpose of the processing and whether the personal identifiable information is being transferred to third parties to be enabled and enforced by the data controller. If the data controller does not comply with a data subject's request within 30 days, the data subject can request the relevant rights to be enforced by the Personal Data Protection Authority. Compensation claims are subject to the jurisdiction of civil courts and criminal complaints to the jurisdiction of criminal courts.

Law stated - 1 June 2024

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

39 Does the law include any derogations, exclusions or limitations other than those already described?

The PDPL does not include any derogations, exclusions or limitations other than those already described.

Law stated - 1 June 2024

SPECIFIC DATA PROCESSING

Cookies and similar technology

40 | Are there any rules on the use of 'cookies' or equivalent technology?

Electronic communications, in general, are regulated by the Information and Communication Technologies Authority (ICTA), established in accordance with the Law on Electronic Communications. Per the Law on Electronic Communications, the ICTA regulates and supervises the processing and protection of personal data acquired via electronic means.

Despite the fact that there is no explicit legislation on the use of cookies or equivalent technology in the Law on Electronic Communications or other legislation, because applicable legislation does not distinguish between the means of obtaining data, any personal data obtained through cookies or similar technology is under the protection of the law, and data controllers must comply with the rules applicable to the processing of personal data when using cookies or similar technology.

That being said, in June 2022, the Data Protection Board (Board) published a Guide Regarding Cookie Applications (the Guide). The Guide clarifies the data controllers and data subjects regarding which type of cookies require explicit consent, and how the data subjects must be informed when they enter a website. Most importantly, the Guide suggests that data controllers are not required to obtain the explicit consent of the data subjects for first-party analytical cookies.

Law stated - 1 June 2024

Electronic communications marketing

41 | Are there any rules on marketing by email, fax, telephone or other electronic channels?

The Law on the Regulation of Electronic Trade regulates the rules and conditions for marketing via electronic means.

For a data controller to use personal data for marketing by any means, the explicit consent of the data subject must be obtained. Data subjects can always, without providing any reason, request the termination of the electronic marketing communications from the data controller. Data controllers are obliged to terminate all electronic communications with data subjects who request termination within three days. Data controllers are also required to take all necessary means to preserve and protect the acquired personal data, and cannot distribute or disclose personal data without the explicit consent of the data subjects.

Furthermore, the provision of services or sale of goods cannot be made subject to the consent to the collection of personal data that is not necessary for the provision of the relevant service or the making of the relevant sale.

The Board has also published guidance regarding electronic communications bearing personal information and deemed it necessary for data controllers to take reasonable measures to verify the contact information declared by the relevant data subjects (eg, sending a verification code or link to the person's registered phone number or email address).

Law stated - 1 June 2024

Targeted advertising

42 | Are there any rules on targeted online advertising?

There are no specific rules or regulations regarding targeted online advertising. However, general principles shall always apply. Since targeted online advertising does not fall under the scope of legitimate processing under the law, personal data can only be processed through the data subject's explicit consent. Likewise, this is the case for online behavioural advertising as well since most of the personal data is collected through cookies for targeted online advertising.

Although there are no regulations or other guidance published by the Board regarding the use of targeting and advertisement cookies, general rules require data controllers to obtain explicit consent from data subjects while the data subjects are using the data controller's website. Thus, targeted online advertising can only be done through the data subject's explicit consent.

Law stated - 1 June 2024

Sensitive personal information

43 | Are there any rules on the processing of 'sensitive' categories of personal information?

As of 1 June 2024, sensitive personal information (personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, clothing choices and habits, trade union membership, health or sex life, criminal conviction and security measures, and biometric or genetic information) may be processed only in the following circumstances:

- where the data subject has given explicit consent for the processing of sensitive personal data;
- processing of sensitive personal data, including health and sexual life data, is permitted by applicable law;
-

processing of sensitive personal data is necessary to protect the life or body integrity of persons who cannot express their consent due to physical impossibility or whose consent is not legally valid;

- processing of sensitive personal data relates to data made public by the data subject and the processing is consistent with the subject's intention to make the data public;
- processing of sensitive personal data is necessary for the establishment, exercise or protection of a right;
- processing of sensitive personal data by persons who are under the obligation of confidentiality, or by authorised institutions and organisations is necessary for the protection of public health, preventative medicine, medical diagnosis, the delivery of treatment and care, and the planning, management and finance of healthcare services;
- processing of sensitive personal data is compulsory to fulfil legal obligations regarding employment, occupational health and safety, social security, social services, or social aid; and
- processing of sensitive personal data is undertaken by foundations, associations and other non-profit organisations or entities established for political, philosophical, religious or union purposes with respect to their current or former members, or persons who are in regular contact with these organisations and entities, where the processing complies with applicable law and their purposes, is limited to their fields of activity and is not disclosed to third parties.

Processing of data must be in compliance with the purposes stated in the data processing notification. If the processor decides to process the data for any reason other than those stated in the data processing notification, a new notification stating the new purpose must be provided to the data subject.

The Board has issued heightened measures for the safekeeping and processing of sensitive personal data. These measures include, among others, training programs, encryption requirements, two-factor authentication for remote access and physical security measures such as access controls.

Law stated - 1 June 2024

Profiling

44 | Are there any rules regarding individual profiling?

There are no specific rules or regulations for individual profiling. However, general principles shall always apply for individual profiling. Thus, if the processing (profiling) is done for commercial purposes, in addition to the duty to inform the data subject regarding the purpose of processing, which data is being processed and whether the data controller is processing personal data through automated means, explicit consent of the data subject must be obtained.

Law stated - 1 June 2024

Cloud services

45 | Are there any rules or regulator guidance on the use of cloud computing services?

Various pieces of legislation apply to the use of cloud computing services: the Universal Services Law; the Electronic Communications Law; the Regulation on Electronic Communications Infrastructure and Information Systems; and the Regulation on Rules on the Operations, Work and Supervision of Data Storage Institutions, among others. Furthermore, the ICTA regulates the use of cloud computing services.

Having said that, the Turkish government's policy preference is the storage of personal data in Turkey.

Law stated - 1 June 2024

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

In March 2024, the Turkish Parliament enacted significant amendments to the PDPL for the first time. These amendments are primarily focused on the processing of sensitive personal data, the transfer of personal data outside of Turkey, and legal remedies against administrative fines imposed by the Board.

With the amendments, new rules were introduced for the processing of sensitive personal data of employees for employment, occupational health and safety purposes. For the transfer of personal data outside of Turkey, three categories of transfer were introduced where firstly, data transfer is possible only to countries, sectors or institutions for which there is adequate protection for the personal data; secondly, if there is no adequacy decision given by the Board, transfer of personal data is permitted by taking the appropriate safeguards in accordance with the PDPL; and lastly, if there is no adequacy decision or taking appropriate safeguards is not possible, temporary, non-repetitive transfers have been made possible, provided that the requirements in the PDPL are met. With the amendments, jurisdiction for legal remedies against administrative fines was transferred from criminal courts of peace to administrative courts. These amendments came into force on 1 June 2024. However, transfers abroad with the explicit consent of the data subject pursuant to the current regulation in the PDPL will continue to be valid, together with the newly available routes, until 1 September 2024.

The Authority and the Board have not yet published a list of countries, sectors within the country or international organisations with adequate protection; have not published the standard contract for the transfer of personal data abroad; and avehave have not published which countries provide data subjects the right to exercise their rights and apply for legal remedies for use of standard contracts. However, in early May 2024, the Authority published the Draft Regulation on the Procedures and Principles Regarding the Transfer of Personal

Data Abroad (Draft Regulation). The Draft Regulation mainly repeats the regulations in the Amendments and regulates the use and signature process of standard contracts for transfer. The Authority is currently seeking comments on the public Draft Regulation, and is expected to publish the final version soon.

Law stated - 1 June 2024

TURUNÇ

Esin Çamlıbel	ecamlibel@turunc.av.tr
Beste Yıldızili Ergül	byildizili@turunc.av.tr
Naz Esen	nesen@turunc.av.tr
Canberk Taze	ctaze@turunc.av.tr

Turunç