ICLG

The International Comparative Legal Guide to:

Data Protection 2015

2nd Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

A.G. Erotocritou LLC
Adsuar Muñiz Goyco Seda & Pérez-Ochoa, P.S.C.
Affärsadvokaterna i Sverige AB
Brinkhof
Cuatrecasas, Gonçalves Pereira
Dittmar & Indrenius
ECIJA ABOGADOS
ELIG, Attorneys-at-Law
Eversheds
Gilbert + Tobin
Gorodissky & Partners
Herbst Kinsky Rechtsanwälte GmbH
Hogan Lovells BSTL, S.C.
Hunton & Williams LLP
Juridicon Law Firm
Jurisconsul
Lee and Li, Attorneys-at-Law
Matheson
Mori Hamada & Matsumoto
Opice Blum, Bruno, Abrusio
& Vainzof Advogados Associados
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi
Portolano Cavallo Studio Legale
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA

GLG
Global Legal Group

GLG
Global Legal Group

Contributing Editor
Bridget Treacy,
Hunton & Williams

Head of Business Development
Dror Levy

Sales Director
Florjan Osmani

Commercial Director
Antony Dine

Account Directors
Oliver Smith, Rory Smith

Senior Account Manager
Maria Lopez

Sales Support Manager
Toni Hayward

Sub Editor
Amy Hirst

Senior Editor
Suzie Levy

Group Consulting Editor
Alan Falach

Group Publisher
Richard Firth

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
May 2015

ISBN
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

Chapter 31

Turkey

Gönenç Gürkaynak

İlay Yılmaz

ELIG, Attorneys-at-Law

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Turkey does not have legislation specifically dedicated to data protection and privacy in effect. However, a number of provisions applicable to data protection and privacy can be found in a variety of Turkish laws, including the Constitution of the Republic of Turkey, and there are certain sector-specific regulations on this matter as well.

Turkey is also a party to the United Nations Universal Declaration of Human Rights and Convention for the Protection of Human Rights and Fundamental Freedoms and has signed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108), but has not yet ratified it.

There is also the Draft Law on the Protection of Personal Data ("Draft Law") which has been pending since 2003. Once the long awaited Draft Law comes into force, it will be the main regulation that sets out the procedures and principles of data protection law in Turkey. Turkish law gives effect to the general principle of *lex specialis*, according to which a special rule dealing with a specific matter prevails over a general rule on the same matter. As a result, the Draft Law, once it has entered into force, would be the primary legal source for – and apply in priority to – matters regarding data protection and privacy. Nevertheless, remaining legal remedies will be applicable for individuals who seek legal remedies regarding data protection and privacy related issues.

The Draft Law was finally submitted to the Turkish Grand National Assembly ("TGNA") on December 26, 2014. Our references to the Draft Law herein are based on the version submitted to the TGNA on December 26, 2014 and might be subject to changes in the future, when the Draft Law enters into force.

1.2 Is there any other general legislation that impacts data protection?

The general provisions that are applicable to data protection and privacy are mainly as follows:

(i) Article 20 (Privacy of Private Life) and Article 22 (Freedom of Communication) of the Constitution of Republic of Turkey (the 'Constitution') dated 9 November 1982;

(ii) Article 24 (Protection of Personality against Violations) of the Turkish Civil Code (the 'Civil Code'); and

(iii) Article 135 (Recording of Personal Data), Article 136 (Unlawfully Disseminating or Capturing Data), Article 138 (Failure to Destroy Data) and Article 244 (Preventing and Impairing the System, Altering or Destroying Data) of the Turkish Criminal Code ("Criminal Code"), which regulate unlawful storage of, transmission, reception or alteration of, destruction or failure to destroy personal data, respectively.

1.3 Is there any sector specific legislation that impacts data protection?

The sector-specific regulations relevant to data protection and privacy are mainly as follows:

(a) Regulation on Procedures and Principles of Broadcasts via Internet and Regulation on Mass Internet Use Providers.

(b) The E-commerce Law.

(c) Regulation on Protection and Sharing of General Health Insurance Data.

(d) Regulation on Data Privacy and Principles and Procedures Regarding Security of Confidential Data in the Official Statistics.

(e) Regulation on Bank Cards and Credit Cards.

(f) Regulation on Distance Contracts.

(g) The Electronic Communications Law and its secondary legislation.

1.4 What is the relevant data protection regulatory authority(ies)?

Currently, there is no specific data protection authority in Turkey. Having said that, the Draft Law stipulates establishment of an independent Board ("Board") for performing the tasks related to personal data assigned to it by the Draft Law and other relevant legislation. Therefore the Board will be the data protection regulatory authority in Turkey when the Draft Law enters into force.

Currently, Turkish courts are entitled to cease unauthorised and/or unlawful processing of personal data. For instance, the courts are entitled to stop the publication and distribution of a person's photograph as injunctive relief.

In addition, there is a special authority for electronic communications in Turkey. Pursuant to the Electronic Communications Law, the Information and Communication Technologies Authority ("ITCA") is responsible for making necessary arrangements and the supervision pertaining to the rights of subscribers, users, consumers and end users, as well as processing of personal data and the protection of privacy. The ITCA exercises its authority

through the Information Technologies and Communication Board (the "ITCB"). There are a significant number of Board decisions imposing general data protection principles on operators in the electronic communications sector.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  Personal data is not defined under Turkish legislation and is defined as per court precedents. The Constitutional Court provided the scope of the definition of "personal data" in its decision of April 9, 2014 as not only the information presenting a person's identity such as name, surname, date of birth, or place of birth but all data directly or indirectly making that person identifiable, including but not limited to a telephone number, motor vehicle licence plate, social security number, passport number, resume, photo, picture, voice records, fingerprints, genetic information, IP address, e-mail address, hobbies, preferences, people that they are in interaction with, memberships, family information.

  On the other hand, according to the definition under the Draft Law, personal data means any information relating to an identified or identifiable natural person.

- **"Sensitive Personal Data"**

  Sensitive personal data is not specifically defined under the Turkish legislation. However, there are certain types of data defined under sector specific legislations which might be deemed sensitive personal data related to these areas.

  In the Regulation on Protection and Sharing of General Health Insurance Data, data regarding the health services provided to a general health insurant and his or her dependants is defined as "medical data". Another type of data regulated under the Regulation on Bank Cards and Credit Cards is "sensitive data regarding cards", which is defined as PIN information that is written on a bank card or credit card which enables financial transactions to be carried out.

  Furthermore the Draft Law also provides a special group of data which is named as "special categories of personal data". According to Article 7 of the Draft Law, the Data concerning the racial or ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, association, foundation or trade-union membership, health or sex life of a person is deemed to be within the scope of special categories of personal data. Special categories of personal data may not be processed, in principle, under the Draft Law.

- **"Processing"**

  According to the Draft Law any operation which is performed on personal data, whether or not by automatic means, such as collection, recording, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction wholly or partly means processing of personal data.

- **"Data Controller"**

  The Draft Law defines the data controller as the real person or legal entity which is in charge of the establishment and management of the data filing system within a unit, institution or agency.

- **"Data Processor"**

  The Draft Law defines the data processor as the real person or legal entity which processes personal data based on the authority given by and on behalf of the controller.

- **"Data Owner"**

  Data owner is not defined under the currently effective Turkish legislation or the Draft Law.

- **"Data Subject"**

  The Draft Law defines the data subject as the real person whose data is processed.

- **"Pseudonymous Data"**

  Pseudonymous data is not defined either under the currently effective Turkish legislation or the Draft Law.

- **"Direct Personal Data"**

  Turkish law does not distinguish direct and indirect personal data.

- **"Indirect Personal Data"**

  Turkish law does not distinguish direct and indirect personal data.

- *Other key definitions*

  The Draft Law defines "anonymising" as rendering personal data anonymous in such a way that it cannot be related to an identified or identifiable natural person.

  Another key definition under the Draft Law is the "data filing system" which is defined as the system structured according to specific criteria in such a way so as to make personal data accessible.

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  The Draft Law imposes obligations on the data controller in order to provide transparency. Accordingly, a data controller is obliged to provide a data subject – about whom data has been collected – with the following information:

  a) the identity of the controller and of his representative, if any;

  b) the purposes of the processing;

  c) to whom the personal data will be transferred and with what purpose;

  d) the method and legal reason for collection; and

  e) other rights as referred to in the Draft Law.

  The data controller is also obliged to inform the data subject when the personal data are erased, destroyed or anonymised.

- **Lawful basis for processing**

  Personal data may be processed if (i) the law allows such processing, or (ii) the data subject whose personal data is being processed explicitly consents to such recording (Article 20 of the Turkish Constitution).

  Furthermore, according to the Draft Law, personal data must be processed lawfully and fairly.

- **Purpose limitation**

  According to the Draft Law, personal data should be (a) kept up to date and only processed for specified, explicit and legitimate purposes, (b) relevant, limited and not excessive in relation to the purposes for which they are processed, and (c) only kept for as long as it is necessitated by the purpose for which they are being processed.

- **Data minimisation**

  The foregoing principles indicated under "Purpose limitation" cover data minimisation as well.

- **Proportionality**

  The foregoing principles indicated under "Purpose limitation" cover proportionality as well.

- **Retention**

  The foregoing principles indicated under "Purpose limitation" cover retention as well.

- *Other key principles*

  According to the Draft Law, personal data should be kept accurate and where necessary kept up to date.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  The Draft Law entitles a person to apply to the data controller and (i) learn whether or not data relating to him are being processed, (ii) request further information if personal data relating to him have been processed, (iii) obtain information as to the purposes of the processing and whether or not data relating to him have been processed accordingly.

- **Correction and deletion**

  The Draft Law entitles a person to (i) ask for the rectification of any incomplete or inaccurate data relating to him, and (ii) ask for the erasure or destruction of the data relating to him. Furthermore, there are conditions as to the erasure or destruction of the data referred to in the relevant article. Accordingly, in the event that the reasons for which personal data are processed are no longer valid, despite being processed in line with the Draft Law or any other related law, personal data should be erased, destroyed or anonymised by the controller *ex officio* or upon the demand of the data subject.

- **Objection to processing**

  The Draft Law entitles a person to object to any consequence to himself which results from the analysis of the processed personal data by means of automated systems.

- **Objection to marketing**

  Turkish law does not provide individuals with a specific right to object to the marketing of personal data.

- **Complaint to relevant data protection authority(ies)**

  According to the Draft Law, the data subject shall communicate to the data controller his claims related to the implementation of the Draft Law in writing or by other means to be identified by the Board. The claims raised in the application are fulfilled by the data controller within the shortest period of time and within a maximum period of thirty days according to the characteristics of the demand, free of charge or, if the operation requires extra costs to be incurred, in return for a fee that is deemed appropriate by the Board or shall be rejected with justifications.

  Furthermore, the data subject may lodge an objection to the Board within thirty days if his application to the data controller is rejected or not responded to by the data controller or if he finds the response to be insufficient.

- *Other key rights*

  The Draft Law entitles data subjects to (i) obtain information as to the third persons within or outside the country to whom data relating to him are transferred, (ii) request the notification to third parties to whom the data have been disclosed of any operation carried out within the scope of his correction or erasure request, and (iii) demand compensation for the damages he has suffered as a result of an unlawful processing operation.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

According to the Draft Law, real persons or legal entities processing personal data must register to the publicly available Registry of Data Controllers ("Registry") before they start processing. However, the Board may provide for an exemption from the obligation to register to the Registry in so far as this is in line with the objective criteria to be determined by the Board such as the characteristics and the number of data to be processed, whether or not data processing is required by law or whether or not data will be transferred to third parties. The registration is made through a notification submitted to the General Secretariat of the Board "Secretariat".

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

The Draft Law does not indicate the basis on which registrations/notifications should be made and refers to the objective criteria to be determined by the Board.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

The Draft Law does not specify the persons who must register with/notify the Secretariat.

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

As per the Draft Law, the notification to be submitted to the Secretariat must include the following information:

a) the name and address of the controller or his representative, if any;

b) the purposes of the processing;

c) a description of the category or categories of the data subject and of the data or categories of data relating to them;

d) the recipients or categories of recipient to whom the data might be disclosed;

e) proposed transfers of data outside of the country; and

f) measures taken to ensure security of personal data.

5.5 What are the sanctions for failure to register/notify where required?

Failure to comply with the registration and notification obligations under the Draft Law is subject to an administrative fine ranging from 10,000 TL to 1,000,000 TL. This administrative fine is imposed on data controllers.

Furthermore any person who stores, keeps, alters, re-organises, discloses, makes accessible, categorises or obstructs the use or transfer of personal data to third parties, other than in accordance with the Draft Law, can be punished in accordance with article 135 of the Criminal Code which reads as follows: "*Whoever unlawfully records personal data shall be imprisoned from one year up to three years.*"

As the Draft Law regulates this sanction in relation to all processing which is contrary to the Draft Law, this provision might be applicable to the data controllers who fail to register/notify pursuant to the Draft Law.

5.6 What is the fee per registration (if applicable)?

The Draft Law does not indicate the registration fees applicable for registration.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

The Draft Law does not regulate renewal of registrations/notifications but requires the data processors to inform the Board of any changes affecting the information provided in the notification.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

The Draft Law requires the data processors to register with the Registry before starting to process data.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

As for the procedures and principles pertaining to the Registry, including the notification and applicable timeframes, the Draft Law refers to the regulation to be issued in the future.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

The Draft Law does not require appointment of a data protection officer. Therefore appointment of a data protection officer can be deemed optional.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Officer where required?

This is not applicable.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

This is not applicable.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

This is not applicable.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

This is not applicable.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, e-mail, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

The Law on Regulation of Electronic Commerce ("E-Commerce Law") requires commercial electronic communications, including spam e-mails, direct marketing calls, call centre calls and SMS marketing messages to be sent to the recipients who are not merchants or artisans, for commercial purposes and through an electric medium, only if their prior consent has been obtained. According to the E-Commerce Law, the contents of commercial electronic messages have to be in compliance with the consent obtained from the recipient.

Having said that, as per Temporary Article 1 of the E-Commerce Law, this provision will not be applied for databases which are established by taking the data subjects' consent before the E-Commerce Law enters into force (i.e. May 1, 2015).

Furthermore, recipients of commercial electronic messages must have the option to opt-out of these marketing communications. Service providers within the scope of E-Commerce (who are defined as real persons or legal entities engaging in electronic commerce activities) are obliged to ensure that the recipients can convey their messages for opting out of these messaging services with ease and without charge.

Moreover, service providers are obliged to provide (i) sufficient information for identifying the real person or legal entity who conducts this communication clearly, and (ii) sufficient and clear information on promotions such as discounts and gifts and promotional contests in order to identify the features, as well as the terms for participation of these promotional activities.

Marketing communications sent through physical means such as communications sent through the post are not within the scope of application of the E-Commerce Law and regulated under the general provisions pertaining to consumer protection with respect to commercials under Turkish laws. There are no specific provisions as to marketing communications sent by physical means to recipients.

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

No. The data protection authority regulated under the Draft Law is not active in enforcement of breaches of marketing restrictions. According to the E-Commerce Law, the Ministry of Customs and Commerce is responsible for enforcement and supervision of the E-Commerce Law.

7.3 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The maximum penalty under the E-Commerce Law for sending multiple recipients electronic marketing communications without obtaining their prior consent is subject to an administrative fine up to ten times the administrative fine ranging from 1,000 Turkish Liras to 5,000 Turkish Liras.

7.4 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

There are no specific requirements for cookies under Turkish legislation. However the general rule requiring prior explicit consent (opt-in) regulated under the Constitution might be applicable for cookies as well. Therefore the data subject's explicit consent would be required for obtaining their data through cookies.

7.5 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

There are no types of cookies where implied consent is acceptable under Turkish legislation.

7.6 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

As there is no data protection authority established in the Turkish jurisdiction, there have been no enforcement actions in relation to cookies.

7.7 What are the maximum penalties for breaches of applicable cookie restrictions?

Unlawfully recording personal data, whether through a cookie or otherwise, is a crime under the Criminal Code. According to the relevant provision, whoever unlawfully records personal data shall be imprisoned from one year up to three years.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad?

The Draft Law regulates transferring personal data abroad and states that "*personal data cannot be transferred to third persons or to a foreign country*". However, consecutive paragraphs regulate the specific circumstances in which personal data can be transferred abroad.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

The Draft Law states that personal data which can be processed without the explicit consent of the data subject can also be transferred abroad without the explicit consent of the data subject on the condition that the recipient country ensures an adequate level of protection.

If the recipient foreign country cannot ensure an adequate level of protection of personal data, personal data can only be transferred (i) upon the explicit consent of the data subject, or (ii) if the data controllers in Turkey and in the recipient foreign country provide a written commitment about adequate protection, together with the authorisation of the Board.

Special categories of personal data can be transferred abroad only if it is explicitly foreseen in laws and the explicit consent of the data subject is present together with the authorisation of the Board.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

The Board's authorisation is required in order to transfer personal data abroad according to the Draft Law.

The Board will decide whether a foreign country can afford an adequate level of protection and whether data transfer will be authorised *per* the Draft Law, after consulting the relevant public administrations and agencies and by assessing the international agreements to which Turkey is a party, the situation of reciprocity related to data transfer between Turkey and the country where personal data will be transferred, the personal data category, as well as the purpose and period of processing for each data transfer operation, the relevant legislation applicable in the country to which data will be transferred and the measures that the data controller in the recipient country commits to provide.

Since the Board is not established yet, the period for authorisation is not foreseeable.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

There is no specific legislation regarding whistle-blowing hotlines under the Turkish legislation.

Since the Board is not established yet, there is no relevant guidance.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

This is not applicable.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

Employers who provide whistle-blower hotlines might be deemed data controllers under the Draft Law. The Draft Law requires real persons or legal entities processing personal data to enroll in the Registry before they start processing.

Since the Board is not established yet, the period for approval is not foreseeable.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

Usage of CCTV is not specifically regulated in Turkish legislation and therefore a separate registration/notification or prior approval is not yet required.

However, CCTV operators might be deemed data controllers under the Draft Law and be subject to the obligations therein.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring is not regulated within Turkish legislation. This subject is controversial among the doctrine and Supreme Court precedents. The Supreme Court points out that the employer has the right to review its employees' business computers and e-mail correspondences.

The Supreme Court decided that the employer is entitled to monitor business computer and e-mail messages at all times and rendered e-mail correspondences obtained through the employer's monitoring as admissible and legitimate. Therefore, the court granted supremacy to the employer's interest in monitoring business computers and e-mail accounts over an employee's right to privacy.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

According to the doctrine, the employee's consent is not required if monitoring the employee's computer and other devices is related to the security and protection of the workplace or third parties' personal rights. The employer is not obliged to gain the employee's consent before monitoring if the employer tries to prevent crimes in the workplace or to protect the company's confidential and commercial data, where the employer does not have another option in order to prevent possible risks or where there is sufficient reason for interference with the employee's private life. Nevertheless, if there is a doubt on the existence of the foregoing circumstances, the employer is required to obtain the employees' prior consent.

If the employment agreements (i) recognise that company infrastructure should only be used for business purposes at all times, and (ii) grant the employer the right to review/transfer business computers' data, or (iii) the company bylaw or regulations enables the employer to undertake such review, the employee's consent is not required.

10.4 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Since employee monitoring is not regulated within Turkish legislation, notifying works councils/trade unions/employee representatives is a subject to be handled under the relevant labour contracts and collective labour agreements.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

This is not applicable.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The processing of personal data in the cloud is also governed by the relevant legislation pertaining to protection of personal data explained in detail in sections 3 and 4 above. Turkish legislation does not differentiate processing of personal data in the cloud from the processing of personal data in general.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The main principle pertaining to processing data is "explicit consent" of the data subject. According to the Draft Law, personal data may not be processed without the data subject's explicit consent or if the data subject objects to such processing. On the other hand, the Draft Law does not provide any form requirements as to obtaining explicit consent. Therefore explicit consent may be obtained through any means.

Although there are no specific contractual obligations to be imposed on a processor who provides cloud-based services, Regulation on Distance Contracts regulates the processes and basic principles of distance contract practices.

The scope of the regulation is limited with distance contracts, which is defined as: "*contracts to which the seller or provider and the consumer entered in, without them physically being at the same location simultaneously within a system created for marketing goods or services via remote communication tools until the contract is entered into including the moment of entry*".

Therefore any processor who operates in Turkey and provides cloud-based services and the relevant contracts online will be obliged to comply with the Regulation on Distance Contracts. This regulation

requires the seller or the provider to store all the data related to their obligations on the right of withdrawal, informing the consumer, delivery and other obligations provisioned under the regulation for three years. Additionally, intermediary actors who mediate the process of a distance contract via remote communication tools are obliged to store all the data on all the transactions between the seller or provider and the consumer for three years and present this data to the relevant authority, institution or consumer upon request.

Therefore processors providing cloud-based services might be deemed obliged to include specific provisions relating to these issues in their distance contracts for their cloud-based services.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The utilisation of big data and analytics is governed by the relevant legislation pertaining to protection of personal data explained in detail in sections 3 and 4. Turkish legislation does not differentiate processing of personal data and utilisation of big data and analytics from processing of personal data in general.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There is no wide-ranging and enveloping data security standardisation in Turkey. However, there are several governmental institutions and initiatives, as well as sector specific regulations regarding data security.

As a governmental step for maintaining cyber security in Turkey, a cabinet decision regarding conducting, managing, and coordinating national cyber security activities came into force on October 20, 2012. Moreover, on June 20, 2013, another decision on the national cyber security strategy and action plan for the years 2013-2014 came into force. Under the decision of October 20, 2012, a Cyber Security Board was established in Turkey. The Cyber Security Board is entitled to determine the governmental precautions regarding cyber security, to approve national cyber security strategies and procedures and principles within this scope and to maintain the national cyber security and coordination.

Sector specific regulations for the telecommunication sector require service providers in the telecommunications sector to obtain a certificate of conformity from ICTA in terms of TS ISO/IEC 27001 standards on establishing, implementing, maintaining and continually improving information security management systems.

The Communiqué on Management of Information Systems in Banks sets the requirements that banks need to follow in terms of cybersecurity.

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

According to the Draft Law, data controllers are obliged to take necessary measures to provide an adequate level of security and required to immediately notify the Board if the personal data is unlawfully obtained by others. The Board declares this situation on its website or via other appropriate means.

The details are not defined under the Draft Law.

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

According to the Draft Law, data controllers are obliged to immediately notify the data subject if their personal data is unlawfully obtained by others.

The details are not defined under the Draft Law.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

According to the Draft Law, the Board is entitled to:

(i) carry out or to have carried out reviews and inspections, *ex officio* or upon complaints, as to whether or not personal data are processed in line with the provisions of the Draft Law;

(ii) take interim measures against the possibility of irrecoverable damages to the data subject;

(iii) issue regulatory acts in areas relating to the processing of personal data;

(iv) co-operate with national and international institutions and agencies in the area of the Draft Law; and

(v) decide on the administrative sanctions foreseen in the Draft Law.

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

This is not applicable.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within Turkey respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Companies operating in Turkey are subject to Turkish legislation in

accordance with sovereignty. Therefore companies in Turkey are not obliged to respond to foreign e-discovery requests or requests for disclosure from foreign law enforcement agencies. However, there are international and bilateral agreements governing exchange of information regarding personal data such as the Hague (Evidence) Convention for Civil Matters, European Convention on Mutual Assistance in Criminal Matters and the Treaty on Extradition and Mutual Assistance in Criminal Matters between the Republic of Turkey and the U.S.

15.2 What guidance has the data protection authority(ies) issued?

This is not applicable.

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

(i) **Constitutional Court's decision of February 14, 2013 and State Council's 15th Chamber Decision of June 12, 2014**

The Constitutional Court cancelled the Decree Law No. 663, which authorised the Ministry of Health to collect, process and disseminate patient data by stating that handling sensitive personal data (healthcare data in this case) cannot be regulated by vesting an authority to an institution.

The State Council's decision is about a circular issued by the Ministry of Health pursuant to Decree Law No. 663, with which the ministry requested all healthcare institutions to provide the Ministry with all patient data. The State Council cancelled the circular by stating that Decree Law No. 663 has been cancelled by the Constitutional Court, therefore the circular has lost its legal ground.

(ii) **Constitutional Court Decision of April 9, 2014**

The Constitutional Court cancelled Article 51 of the Electronic Communications Law which authorised ICTA to regulate the principles and procedures for the processing of and protecting of privacy of personal data in the electronic communications sector by stating that the procedures and basics for protection of personal data can only be regulated by law pursuant to Article 20 of the Constitution.

(iii) **Ombudsman Decision of November 26, 2014 with Application Number 03.2013/54, Decision Number 2013/83**

The application subject to the Ombudsman's decision was about personal data stored in criminal records databases. The applicant stated that his crime records regarding crimes he committed when he was 14 were still accessible by law enforcement officers when his criminal records were checked via the law enforcement database of the Ministry of Interior Affairs although this data has been removed from his criminal records many years ago. The applicant claims that his personal data is stored *as per* a regulation issued by the Ministry of Interior Affairs. The applicant requested from the Ombudsman that his personal data stored in the Ministry of Interior Affairs' databases be deleted.

The Ombudsman discussed if the regulation complies with Convention 108, as well as Article 20 of the Constitution and stated that: "*it is unclear under what conditions, for how much time, for what purposes the personal data is stored pursuant to the directive; therefore the balance between the protection of a person's material and spiritual being, basic human rights and processing, recording, disseminating and storing personal data and no necessary precautions against abusive behaviors have been taken and no efficient audit mechanisms have been established to prevent misuse, the legal boundaries for the evaluation of personal data have not been established*".

The Ombudsman further stated that regulating the conditions, term and deletion of criminal records of persons under a regulation without establishing certain boundaries within a law might incur serious restriction on basic human rights and is against Article 20 of the Constitution and does not comply with the principle of proportionality.

The Ombudsman finally advised the government to establish dedicated data protection legislation by ratifying the Draft Law.

16.2 What "hot topics" are currently a focus for the data protection regulator?

The hottest topic for the Turkish government and the TGNA in terms of protection of personal data is national security. National security became a concern as a result of leaked wire-tappings in December 2013. These tappings included recordings of telephone conversations between the highest ranking government officials, well-known businessman and members of the press. As a result, the Draft Law is being introduced as part of the legislative package on internal security. This approach is materialised within the Draft Law in the form of wide and vague exemptions provided for governmental agencies. Although the Draft Law is based on the Directive 95/46/EC, the two legislations differ in terms of their aims regarding these exemptions. While the Draft Law appears to be aiming to grant the governmental bodies a form of immunity when protection of personal data is concerned, Directive 1995/46/EC provides these exemptions are limited to the context of the data subject's right to information and aims to strengthen the rule of law and accountability of governmental bodies.

Gönenç Gürkaynak
ELIG, Attorneys-at-Law
Yildiz Mahallesi, Citlenbik Sokak No: 12
Besiktas
Istanbul
Turkey

Tel: +90 212 327 1724
Fax: +90 212 327 1725
Email: gonenc.gurkaynak@elig.com
URL: www.elig.com

Mr. Gönenç Gürkaynak is a founding partner and the managing partner of ELIG, Attorneys-at-Law, a firm of 55 lawyers based in Istanbul, Turkey. Mr. Gürkaynak graduated from Ankara University Faculty of Law in 1997 and was called to the Istanbul Bar in 1998. Mr. Gürkaynak received his LL.M. degree from Harvard Law School and is qualified to practise law in Istanbul, New York, Brussels, and England and Wales (as a non-practising solicitor). Before founding ELIG, Attorneys-at-Law in 2005, Mr. Gürkaynak worked as an attorney at the Istanbul, New York and Brussels offices of a global law firm for more than eight years.

Mr. Gürkaynak heads the significant media, internet and telecommunications law practice at ELIG, Attorneys-at-Law. Mr. Gürkaynak has successfully represented multinational companies and key domestic clients before the Constitutional Court and the Administrative Courts and provides advice on a range of matters.

İlay Yılmaz
ELIG, Attorneys-at-Law
Yildiz Mahallesi, Citlenbik Sokak No: 12
Besiktas
Istanbul
Turkey

Tel: +90 212 327 1724
Fax: +90 212 327 1725
Email: ilay.yilmaz@elig.com
URL: www.elig.com

Ms. İlay Yılmaz is partner of ELIG, Attorneys-at-Law. She joined ELIG in 2008, following her years of practice at reputable law firms. Ms. Yılmaz graduated from Dokuz Eylul University Faculty of Law in 2003 and is admitted to the İstanbul Bar. She is currently studying to gain her LL.M. degree from Bilgi University. Her practice focuses on Internet law, IT and telecommunications law, media and entertainment law, data protection law, contracts law, energy market law and general corporate law. Ms. Yılmaz has authored and co-authored many articles and essays pertaining to her practice areas, in addition to speaking at conferences and symposia on similar matters.

ELİG
Attorneys at Law

ELIG is committed to providing its clients with high-quality legal services. We combine a solid knowledge of Turkish law with a business-minded approach to develop legal solutions that meet the ever-changing needs of our clients in their international and domestic operations.

We have a legal team of 55 people. While ELIG lawyers have the knowledge and experience to assist clients in almost all fields of law, ELIG's core strengths are corporate law, mergers & acquisitions, competition law, EU law, banking and finance, litigation, IT, media and telecommunications law, Internet law, data protection and privacy law, energy, oil and gas law, administrative law, real estate law, white collar irregularities, and intellectual property law.

As an independent Turkish law firm, ELIG collaborates with many international law firms on various projects.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Recovery & Insolvency
- Corporate Tax
- Data Protection
- Employment & Labour Law
- Environment & Climate Change Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Litigation & Dispute Resolution
- Lending & Secured Finance
- Merger Control
- Mining Law
- Oil & Gas Regulation
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks

GLG
Global Legal Group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: sales@glgroup.co.uk

www.iclg.co.uk