LATEST EDITION

Comparing privacy laws:
GDPR v. LPPD

April 2023

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

Esin Attorney Partnership.

About the authors

OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk, and achieve global compliance.

OneTrust DataGuidance™ regulatory research includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Comparisons which allow you to compare regulations across multiple jurisdictions at a glance, a daily customised news service, and expert analysis. These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy program.

Esin Attorney Partnership: A member firm of Baker & McKenzie International, a Swiss Verein, provides clients with outstanding foreign and Turkish law advice.

Esin Attorney Partnership has been named Turkey Law Firm of the Year at the Chambers Europe Awards in 2021, Turkey Banking & Finance Firm of the Year at the IFLR Europe Awards 2021, Turkey M&A Legal Advisor of the Year by the Mergermarket Europe Awards 2020, Turkey Law Firm of the Year by the IFLR European Awards in 2020, Diversity & Inclusion Firm of the Year by the International Tax Review in 2020; Turkey Tax Firm of the Year by the International Tax Review in 2019 and 2020, Turkey Law Firm of the Year at the Chambers Europe Awards 2018; Turkey Most Innovative Law Firm of the Year at the IFLR European Awards 2018; Legal Adviser of the Year in Turkey at the European M&A Awards in 2016 and 2010 by the Financial Times and Mergermarket showing our long history of top-quality legal work..

Contributors

OneTrust DataGuidance™: Angela Potter, Bahar Toto, Alahi Kazi, Rhiannon Gibbs-Harris, Matteo Quartieri, Amelia Williams, Lea Busch, Suzanna Georgopoulou, Marina Ioannou, Gabriel Negoita, Victoria Ashcroft, and Angus Young

Esin Attorney Partnership: İlay Yılmaz, Can Sözer, Ecem Elver

Image production credits:

Cover/p.5/p.51: cnythzl / Signature collection / istockphoto.com
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com
Icon p.12-21: Moto-rama / Essentials collection / istockphoto.com
Icon p.22-23: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.25, 29-37: zak00 / Signature collection / istockphoto.com
Icon p.38-45: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.47-51: cnythzl / Signature collection / istockphoto.com

Table of contents

Introduction

On 25 May 2018, the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') came into effect and replaced the Data Protection Directive (Directive 95/46/EC). The Law on Protection of Personal Data No. 6698 ('the LPPD') was published in the Official Gazette of Turkey on 7 April 2016, numbered 29677 and entered into force. The LPPD is the first general data protection law in Turkey and is largely based on the former European Data Protection Directive. Secondary legislation introduced in Turkey in the form of regulations and communications have, though, led to a similar development as the changes in the EU brought about by the GDPR.

There are several areas in which the GDPR and the LPPD bare a strong similarity, including, for instance, their material scope. Both the GDPR and the LPPD provide comparable definitions for key concepts such as 'processing', 'personal data' and 'sensitive data', and apply to the processing of personal data by automated means or non-automated means if the data forms part of a filing system. In addition, the GDPR and the LPPD correspond in respect of the general responsibilities they set out for both data controllers and data processors, such as obligations relating to several data subject rights, data breach notifications, and data security measures. These parallels are particularly close in some instances; for example, both the GDPR and the LPPD provide for a 72-hour timeframe for a breach notification to the competent supervisory authority.

Nevertheless, there are some key differences between the GDPR and the LPPD. In particular, while the GDPR expressly provides that data controllers and data processors maintain a record of the processing activities, the LPPD does not establish such an obligation. The LPPD, however, and unlike the GDPR, requires data controllers to register in the Data Controller's Registry System ('VERBIS'). In their application to VERBIS, data controllers subject to the LPPD must provide information similar to that which data controllers are required to include in their records of processing activities under the GDPR.

Further differences can be found in relation to requirements for Data Protection Impact Assessments ('DPIAs'), data protection officers ('DPOs'), children's data, and pseudonymised data. The LPPD is also less explicit than the GDPR in relation to its extraterritorial scope and provides a more varied set of mechanisms for cross-border data transfers.

This Guide aims to highlight the similarities and differences between the GDPR and the LPPD to assist organisations in their compliance with both.

Structure and overview of the Guide

This Guide provides a comparison of the two pieces of legislation on the following key provisions:

1. Scope
2. Key definitions
3. Legal basis
4. Controller and processor obligations
5. Individuals' rights
6. Enforcement

Each topic includes relevant provisions from the two legislative frameworks, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the LPPD.

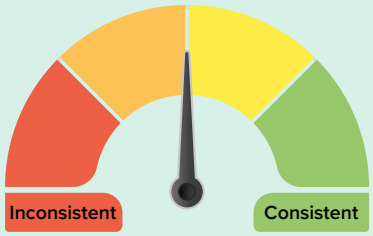
Key for giving the consistency rate

Consistent: The GDPR and the LPPD bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.

Fairly consistent: The GDPR and the LPPD bear a high degree of similarity in the rationale, core, and the scope of the provision considered, however, the details governing its application differ.

Fairly inconsistent: The GDPR and the LPPD bear several differences with regard to the scope and application of the provision considered, however, its rationale and core presents some similarities.

Inconsistent: The GDPR and the LPPD bear a high degree of difference with regard to the rationale, core, scope, and application of the provision considered.



Usage of the Guide

This Guide is general and educational in nature and is not intended to provide, and should not be relied on, as a source of legal advice. The information and materials provided in the Guide may not be applicable in all (or any) situations and should not be acted upon without specific legal advice based on particular circumstances.

1. Scope

Fairly consistent

1.1. Personal scope

Both the GDPR and the LPPD apply to data controllers and data processors, and provide similar definitions for these concepts. Furthermore, both pieces of legislation aim to protect living, natural persons by regulating the activities of public and private bodies.

GDPR	LPPD
Articles 3, 4(1) Recitals 2, 14, 22-25	Articles 1(1), 2(1), 3(1)

Similarities

GDPR	LPPD
The GDPR defines a **data controller** as a 'natural and legal person, public authority, agency or other body which, alone or jointly, with others, determines the purposes and means of the processing of personal data.'	The LPPD defines a **data controller** as a 'natural or legal person who determines the ends and means of the processing of personal data and who is responsible for the establishment and management of the data filing system.'
The GDPR defines a **data processor** as a 'natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.'	The LPPD defines a **data processor** as a 'natural or legal person who processes personal data based on the authority granted by the controller on his behalf.'
Article 4(1) of the GDPR clarifies that a **data subject** is 'an identified or identifiable natural person.'	The LPPD defines a **data subject** as 'a natural person whose personal data are processed.'
The GDPR **applies** to data controllers and data processors who may be **public bodies**.	As there is no distinction between private corporations and public authorities within Turkish law, rules and procedures determined by the LPPD **apply to all institutions and organisations**.
The GDPR **only protects living individuals**. The GDPR does not protect the personal data of deceased individuals, this being left to Member States to regulate.	The LPPD applies to **natural persons** whose personal data are processed. The LPPD does not cover information regarding deceased persons.

Differences

GDPR	LPPD
The GDPR provides that it 'should apply to natural persons, **whatever their nationality or place of residence**, in relation to the processing of their personal data.'	The LPPD does **not** explicitly refer to the nationality or place of residence of data subjects. Instead, it broadly applies to '**natural persons located in Turkey whose personal data are processed**'.

1.2. Territorial scope

While the LPPD does not directly refer to its territorial scope, it can be taken as having similarities to the GDPR and particularly in terms of having a potential extraterritorial applicability.

GDPR	LPPD
Articles 3, 4, 11 Recitals 2, 14, 22-25	Article 2

Similarities

In relation to **extraterritorial scope**, the GDPR applies to the processing activities of data controllers and data processors that **do not have any presence in the EU**, where processing activities are related to the **offering of goods, or services to individuals in the EU, or to the monitoring of the behaviour of individuals in the EU**.

In relation to **extraterritorial scope**, it is accepted that the LPPD applies to the processing of personal data of data subjects located in Turkey, regardless of the location of the data controller/data processor (i.e. located in or outside of Turkey).

Differences

The GDPR does **not** establish a requirement for data processing registration.

The LPPD requires data controllers, **whether based in Turkey or not**, to register with the KVKK's VERBIS, prior to processing any personal data originating in Turkey.

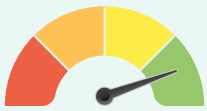
The GDPR **applies** to organisations that have presence in the EU. In particular, Article 3 of the GDPR applies to entities or organisations established in the EU, notably entities that have an '**establishment**' in the EU or if processing of personal data takes place in the context of the activities of that establishment, irrespective of whether the data processing takes place in the EU or not.

The LPPD does not specifically address whether it only applies to companies established in Turkey or whether it has extraterritorial application. However, in line with the principle of territoriality and the application of the provisions of the Criminal Code Law No. 5237 ('the Criminal Code') referred to by Article 17 of the LPPD, **the LPPD shall apply to all natural and legal persons who process personal data originating in Turkey**, regardless of whether data controllers are located in Turkey or abroad.

The GDPR specifically applies extraterritorially where processing activities are related to the **offering of goods, or services to individuals in the EU, or to the monitoring of the behaviour of individuals in the EU**.

Although the LPPD **remains silent on its extraterritorial scope** in terms of the origin of data, by interpretation it is accepted that it applies to data processing activities related to personal data originating in Turkey.

1.3. Material scope



Both the GDPR and the LPPD provide similar definitions for 'processing', 'personal data,' and 'sensitive data', and apply to the processing of personal data by automated means or non-automated means if the data is part of a filing system. In addition, both the GDPR and the LPPD provide for similar exclusions in their application, including processing of personal data in the context of household activities, public security, or law enforcement. Like the GDPR, the LPPD excludes anonymous data.

GDPR	LPPD
Articles 2-4, 9, 26 Recitals 15-21, 26, 27	Articles 1-4, 6, 12, 28(1)

Similarities

The GDPR applies to the '**processing**' of personal data. The definition of 'processing' covers 'any operation' performed on personal data 'such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'	The LPPD applies to the '**processing'** of personal data. The definition of 'processing' covers 'any operation' which is performed upon personal data such as 'collection, recording, storage, preservation, alteration, adaptation, disclosure, transmission, retrieval, making available for collection, categorisation or blocking its use, wholly or partly by automatic means or by other means provided that they form part of a filing system'.
The GDPR defines '**personal data**' as 'any information' that directly or indirectly relates to an identified or identifiable individual. The GDPR does not apply to the personal data of deceased persons.	The LPPD defines '**personal data**' as 'any kind of information relating to an identified or identifiable person.'
The GDPR applies to the processing of personal data **by automated means or non-automated means if the data is part of a filing system**.	The LPPD applies to the processing of personal data **by automated means or non-automated means if the data is part of a filing system**.
The GDPR defines **special categories of personal data** as personal data revealing **racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation**. The GDPR also provides specific requirements for its processing.	Data revealing **racial, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance or dress, membership of an association, foundation or trade union, health, sex life, conviction and security measures and the biometrics and genetics of persons constitute special categories of personal data** under the LPPD. Specific requirements for its processing also apply.
The GDPR **excludes** from its application the processing of personal data by individuals for **purely personal or**	The LPPD **excludes** from its application the processing of personal data by individuals in the course of a

GDPR	LPPD
Similarities (cont'd)	
household purposes. This is data processing that has 'no connection to a professional or commercial activity.'	'**merely personal or household activity**, provided that obligations relating to data security are complied with and data are not transferred to third parties.'
The GDPR **excludes** from its application data processing in the context of **law enforcement or national security**.	The LPPD excludes from its application data processing in the context of preventive, protective, and intelligence-related activities by public institutions and organisations, and by **judicial authorities and execution agencies** with regard to investigation, prosecution, adjudication, or execution procedures.
The GDPR provides requirements for specific processing situations including processing for **journalistic purposes and academic, artistic, or literary expression**.	The LPPD excludes from its application the processing of personal data for the purposes of **art, history, and literature or science**, or within the scope of freedom of expression, provided that national defence, national security, public safety, public order, economic safety, privacy of personal life, or personal rights are not violated.
The GDPR excludes **anonymous data** from its application, which is defined as information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	The LPPD also excludes **anonymous data** from its application, which is defined as personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable, even when matching them with other data.
Differences	
Not applicable.	Not applicable.

2. Key definitions

2.1. Personal data

The GDPR and the LPPD provide similar definitions for 'personal data' and 'sensitive personal data'. Unlike the LPPD, though, the GDPR also specifically provides that IP addresses, cookie identifiers, and radio frequency identification tags may be considered personal data.

GDPR	LPPD
Articles 4(1), 9 Recitals 26-30	Articles 3, 6

Similarities

The GDPR defines '**personal data**' as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'

The LPPD defines '**personal data**' as any information relating to an identified or identifiable natural person ('data subject'). In order for data to be considered as personal data, it has to be related to a natural person who is or can be identified.

The GDPR defines **special categories of personal data** as data revealing a data subject's 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.'

The LPPD defines **special categories of personal data** as personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership of associations, foundations or trade-unions, information relating to health, sexual life, convictions and security measures, and biometric and genetic data. Categories of sensitive personal data are limited by law and thus cannot be extended by interpretation.

The GDPR **does not** apply to 'anonymised' data, where the data can no longer be used to identify the data subject.

The LPPD **does not** apply to 'anonymised' data, where the data can no longer be used to identify the data subject.

Differences

The GDPR specifies that **online identifiers** may be considered as personal data, such as **IP addresses, cookie identifiers, and radio frequency identification tags**.

The LPPD **does not** explicitly specify that online identifiers may be considered personal information. This said, with its decision dated 27 February 2020 and numbered 2020/173, the KVKK has ruled that, to the extent personal data is being processed via cookies, such cookies will be accepted as personal data and usage of such cookies requires data subject's explicit consent. In this vein, the decision no. 2022/229 dated 10 March 2022 of the KVKK also underlined that explicit consents of the data subjects must be obtained for the cookies used for profiling purposes.

2.2. Pseudonymisation

The GDPR provides a definition for pseudonymised data and clarifies that such data are subject to the obligations of the GDPR. The LPPD does not explicitly refer to pseudonymised data.

GDPR	LPPD
Articles 4(5), 11 Recitals 26, 29	Not applicable

Similarities

GDPR	LPPD
Not applicable.	Not applicable.

Differences

GDPR	LPPD
The GDPR defines **pseudonymised data** as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.'	The LPPD does **not** define pseudonymised data.

2.3. Controllers and processors

The GDPR and the LPPD are similar with regard to the scope and responsibilities they set out for data controllers and data processors, and include corresponding definitions and obligations regarding compliance with data subject rights, data breach notifications, and security measures. The KVKK introduced the concept of DPO with the Communiqué on the Procedures and Principles Regarding the Personnel Certification Mechanism dated 6 December 2021 ('Communiqué on the Procedures and Principles Regarding the Personnel Certification Mechanism'). However, appointment of DPO is not a requirement.

Both the GDPR and the LPPD require data controllers to implement appropriate security measures and notify supervisory authorities of data breaches. The GDPR also specifically provides that a Data Protection Impact Assessment ('DPIAs') be conducted in certain circumstances, whereas the LPPD has no directly equivalent concept.

GDPR	LPPD
Articles 4, 17, 28, 30, 32, 33, 35, 37, 38 Recitals 64, 81, 90, 93	Articles 3, 4, 12, 16 Articles 5 and 9 of the Regulation on Data Controllers Registry

Similarities

A **data controller** is a natural or legal person, public authority agency or other body that determines the **purposes** and **means** of the processing of personal data, alone or jointly with others.

The LPPD defines **data controllers** as 'natural or legal persons who determine the **intended purposes** and **means** of processing personal data and who are responsible for **establishing and managing the data registry system**.'

A **data processor** is a natural or legal person, public authority, agency or other body which processes personal data on **behalf** of the controller.

A **data processor** is a natural or legal person who processes personal data on **behalf of and with the authorisation** of the data controller.

Data controllers must comply with the **purpose limitation and accuracy principles, and rectify** a data subject's personal data if it is **inaccurate** or **incomplete**.

According to the LPPD, personal data processing must be **accurate**, and where necessary, kept **up to date**, **relevant**, **limited**, and **proportional** to the purposes of processing, and recorded no longer than is stipulated under the laws or the purposes for which the data was collected.

Data controllers must implement **technical and organisational security measures**, and notify supervisory authorities of **data breaches**.

Data controllers must implement **technical and organisational security measures**, and notify supervisory authorities of **data breaches**.

Data controllers based outside the EU and involved in certain forms of processing, with exceptions based on the scale of processing and type of data, are obliged to **designate a representative based within the EU** in writing.

Data controllers based outside Turkey are obliged to **register** with VERBIS and to **appoint** a **data controller representative** in Turkey to complete the registration process. Foreign data controllers can complete VERBIS registration merely through a data controller representative, which can be a **real or legal person resident in Turkey**.

GDPR	LPPD

Similarities (cont'd)

The GDPR stipulates that data controllers and data processors keep **records of processing activities** and provides an exception from this obligation for small organisations.	The LPPD explicitly requires data controllers (who have the obligation to register with VERBIS) to prepare a personal **data processing inventory**, and a **personal data retention and deletion policy**.

Differences

The GDPR provides that a data controller or data processors conduct **DPIAs** in certain circumstances.	The LPPD does **not** expressly provide for DPIAs. This said, the LPPD holds data controllers responsible for carrying out (or have third parties carry out) necessary audits to ensure compliance with the LPPD within their own organisations.
The GDPR provides for the designation of a **DPO** by data controllers or data processors.	The LPPD does **not require** the appointment of a DPO.
Data controllers are **not** obliged to notify their data processing activities under the GDPR.	The LPPD imposes on data controllers the **obligation to notify their data processing activities** with the KVKK (i.e. to register to the data controllers' registry) with certain exemptions.
The GDPR outlines that data processors shall not engage another data processor without prior specific or general written **authorisation** of the controller.	The LPPD does not establish a written authorisation requirement. However it does specifically **prohibit** processors from disclosing or using the personal data obtained from the controller for purposes other than the initial processing purpose.

2.4. Children

Fairly inconsistent

Unlike the GDPR, the LPPD does not grant special protection to children's personal data, nor does it specify whether the consent of a parent or guardian is needed when processing children's data. Additionally, the brochure regarding processing of children data published by the KVKK on 23 April 2020 ('the Brochure') bears similarities with the GDPR in relation to protective measures and children's right to be informed.

GDPR	LPPD
Articles 6, 8, 12, 40, 57 Recitals 38, 58, 75	The Brochure

Similarities

GDPR	LPPD
The GDPR **does not** define 'child' or 'children.'	The LPPD **does not** define 'child' or 'children.'
The GDPR considers children as '**vulnerable natural persons**' that merit specific protection with regard to their personal data. In particular, specific protection should be given when children's personal data is used for marketing or collected for information society services offered directly to a child.	The LPPD **does not** provide limitations and/or requirements specific to protection of children's personal data. This being said, the Brochure states that data controllers should take technical and **administrative measures with the highest standards** to protect children's personal data.
When any information is addressed specifically to a child, controllers must take **appropriate measures** to provide **information** relating to processing in a concise, transparent, intelligible and **easily accessible form, using clear and plain language, that the child can easily understand**.	The LPPD requires controllers to inform **all data subjects** on data processing activities. In addition, the KVKK states in the Brochure that the privacy notices addressed to children should be in **plain language** and should be **easy to understand from a child's perspective**.

Differences

GDPR	LPPD
Where the processing is based on consent, the consent of a parent or guardian is required for providing information society services to a child below the **age of 16**. EU Member States can **lower this age limit to 13**.	The LPPD does **not** specify whether consent of a parent is required for providing information society services to a child. **The LPPD does not set an age limit for consent**.
The GPDR provides that data controllers are required to make reasonable efforts to **verify** that **consent** is given or authorised by a parent or guardian.	The LPPD does **not** include a specific provision on verification of parent/guardian's consent.
The GDPR applies to **information society services**.	The LPPD does not include specific provisions on **information society services**.

2.5. Research

Fairly inconsistent

Both the GDPR and the LPPD address the processing of personal data for research purposes. This said, the provisions for data processing for research purposes are more detailed under the GDPR than the LPPD.

GDPR	LPPD
Articles 5(1)(b), 9(2)(j), 14(5), 17(3), 21(6), 89 Recitals 33, 159-161	Article 28

Similarities

According to the GDPR, **the processing of sensitive data is not prohibited when 'necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.'

The LPPD is not applicable when personal data is processed for **artistic, historical, literary**, or **scientific purposes** or within the scope of freedom of expression, provided that **national defence, national security, public security, public order, economic security, right of privacy, or personal rights are not violated** or the processing does not constitute a **criminal offence**. The LPPD will not apply to processing activities for **official statistics and research, planning, and statistical purposes**, after having been **anonymised**.

Differences

The data subject has the **right to object** to the processing of personal data for research purposes **unless such research purposes are for reasons of public interest**.

The LPPD does **not** include an objection right specific to processing for research purposes.

Under the GDPR, the processing of personal data for research purposes is subject to **specific rules** (e.g. with regard to the purpose limitation principle, right to erasure, data minimisation and anonymisation etc.).

There are **no** rules under the LPPD specific to processing for research purposes.

The GDPR clarifies that the processing of personal data for **scientific research** purposes should be interpreted 'in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.'

The LPPD does **not** provide an interpretation or definition of scientific research.

Under the GDPR, where personal data are processed for research purposes, it is possible for Member States to derogate from some data subjects' rights, including the right to access, the right to rectification, the right to object and the right to restrict processing, insofar as such rights are likely to render impossible or seriously impair the achievement of the specific purposes.

Under the LPPD, there are **no** derogations for data subjects' rights when the processing is for research purposes.

3. Legal basis

Both the GDPR and the LPPD include provisions in relation to the legal basis for the processing of personal data. In particular, consent, legal obligations, the vital interest of the data subject or another person, the performance of a contract, the exercise of a right, and legitimate interests of the data controller are considered legal bases for processing personal data under both regulations.

In addition, the LPPD provides that processing is lawful when the data has been made public by the data subject and stipulates that consent must be explicit. However, unlike the GDPR, the LPPD does not provide special rules regarding the processing of children's data.

GDPR	LPPD
Articles 5-10 Recitals 39-48	Articles 5, 6

Similarities

The GDPR states that data controllers can only process personal data when there is a legal ground for it. The legal grounds are:

- **consent**;
- when processing is necessary for the **performance of a contract** which the data subject is part of in order to take steps at the request of the data subject prior to the entering into a contract;
- compliance with **legal obligations** to which the data controller is subject;
- to protect the **vital interest** of the data subject or of another natural person;
- performance carried out in the **public interest** or in the official authority vested in the data controller; or
- for the **legitimate interest** of the data controller when this does not override the fundamental rights of the data subject.

Further permissible uses are provided for the processing of special categories of personal data under Article 9(2).

The GDPR recognises **consent** as a legal basis to process personal data. Under the GDPR, as a general rule, the processing of **special categories of personal data is restricted unless** an exemption applies, which include the data subject's **explicit consent**.

The LPPD provides that personal data cannot be processed without the **explicit consent** of the data subject unless one of the following conditions apply:

- it is expressly provided by the **laws**;
- it is obligatory to **protect the life or physical integrity of the data subject or of another person** who is physically incapable of giving their consent or whose consent is not deemed to be legally valid;
- it is necessary to process the personal data of the parties to a contract, provided that processing is directly related to the **conclusion or performance of the contract**;
- it is obligatory for the controller to be able to fulfil its **legal obligation**;
- it is obligatory to process data for the purposes of the **legitimate interests** of the controller, provided that the processing does not prejudice the fundamental rights and freedoms of the data subject;
- it is obligatory to process data for the establishment, exercise, or protection of a **right**; or
- if the data has been **made public by the data subject**.

The LPPD further **prohibits the processing of special categories of personal data without the explicit consent** of the data subject, and that adequate measures, as determined by the Board of the KVKK, shall be taken while processing special categories of personal data.

Similarities (cont'd)

There are specific **legal grounds for processing special categories of data**.

Under the LPPD, **sensitive data** excluding those relating to health and sexual life can be **processed only under the conditions set out by the law**. Personal data relating to health and sexual life may only be processed, without explicit consent of the data subject, by persons under an obligation of confidentiality or by authorised institutions and establishments for the purposes of protection of public health, protective medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

The GDPR includes **specific information** on how consent must be obtained and withdrawn.

The LPPD also includes **specific information** on how consent must be obtained. The LPPD does not explicitly provide individuals with a right to withdraw their consent to the processing of their personal information at any time. However, **by interpretation** of its provisions, it is clear that **data subjects shall have the right to withdraw their consent** to the processing of their personal data at any time.

Differences

The GDPR **provides** information in relation to the conditions applicable to **children's** consent in relation to information society services.

The LPPD does **not** provide special rules regarding the processing of **children's** data. This being said, the Brochure states that data controllers should take technical and **administrative measures with the highest standards** to protect children's personal data and that the privacy notices addressed to children should be in plain language and should be **easy to understand from a child's perspective**.

4. Controller and processor obligations

4.1. Data transfers

Fairly inconsistent

Both the GDPR and the LPPD provide requirements for the transfer of personal data to third countries. The LPPD considers the consent of the data subject as the main legal basis for any overseas transfer. However, both pieces of legislation recognise the concept of adequacy, as well as other legal bases for the transfer of personal data.

The KVKK published a statement on binding corporate rules ('BCRs'), which states that in the event that adequate protection is not provided in the country to which personal data to be transferred, such data may be transferred abroad without explicit consent of the data subject upon the existence of commitment for adequate protection in writing by the data controllers in Turkey and authorisation of the Board. That said, the Economical Reform Action Plan set the date for LPPD's cross-border transfer mechanisms alignment with GDPR as 31 March 2022. Although, there is no official amendments introduces or submitted to the Turkish Grand National Assembly, there may be certain changes in LPPD in future, especially affecting the cross-border transfer mechanisms.

GDPR	LPPD
Articles 44-50 Recitals 101, 112	Articles 5(2), 6(3), 9 KVKK statement on Binding Corporate Rules ('BCR')

Similarities

The GDPR allows personal data to be transferred to a third country or international organisation that has an **adequate level of protection** as determined by the EU Commission.

One of the following legal grounds can be applied to the transfer of personal data abroad:

- prior **consent**
- when a data subject has explicitly **consented** to the proposed transfer and acknowledged the possible risks of such transfer due to inadequate safeguards;
- when the transfer is necessary for the performance or conclusion of a **contract**;
- when the transfer is necessary for important **public interest** reasons;
- when the transfer is necessary for the establishment, exercise, or defence of a **legal** claim; and
- when the transfer is necessary to protect the **vital interests** of a data subject or other persons.

The LPPD establishes that personal data cannot be transferred overseas without the explicit consent of the data subject, unless the receiving country provides an **adequate level of protection** and certain other grounds are met. The countries where an adequate level of protection is provided have not been determined and declared yet by the Board of the KVKK.

Provided that an adequate level of protection is provided in the foreign country where personal data are to be processed, data can be transferred overseas without the explicit consent of the data subject in the following cases:

- the transfer is expressly provided by the **law**;
- the transfer is **necessary** in order to protect the life or physical integrity of the data subject or of another person who is physically incapable of providing their consent, or whose consent is not deemed to be legally valid;
- the transfer is necessary in order to process the personal data of the parties to a **contract**, provided that the processing is directly related to the conclusion/performance of the contract itself;
- the transfer is necessary for the controller to be able to fulfil its **legal obligation**;
- data has been **made public** by the data subject;

Similarities (cont'd)

- it is obligatory to process data for the establishment, exercise, or **protection of a right**;
- it is obligatory to process data for the purposes of the **legitimate interests** of the controller, provided that the processing does not prejudice the fundamental rights and freedoms of the data subject; or
- provided that adequate measures are taken, personal data other than those revealing health and sex life provided in Article 6(1) of the LPPD can be processed without explicit consent of the data subject in cases prescribed by the law. Personal data relating to health and sexual life, provided that it is transferred by persons under an obligation of confidentiality or by authorised institutions and establishments for the purposes of protection of public health, protective medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

In the absence of a decision on adequate level of protection, a transfer is permitted when **the data controller or data processor provides appropriate safeguards** with effective legal remedies that ensure the data subjects' rights as prescribed under the GDPR. **Appropriate safeguards include**:

- BCRs with specific requirements (e.g. a legal basis for processing, a retention period, complaint procedures, etc.);
- standard data protection clauses adopted by the EU Commission or by a supervisory authority;
- an approved code of conduct; or
- an approved certification mechanism.

In addition, the KVKK has specified that **BCRs** represent an **additional mechanism** that may be used to facilitate international data transfers as per Article 9 of the LPPD. Specifically, BCRs are defined as mechanisms used for the transfer of personal data abroad for multinational group companies operating in countries where adequate protection is not available. The KVKK further outlined that BCRs are subject to the permission of the Board of the KVKK. After the application for permission, the Board of the KVKK has a one year term to finalise the application and this one-year term can be extended by the Board of the KVKK in six month intervals.

Differences

The GDPR specifies that a cross-border transfer is allowed based on **international agreements** for judicial cooperation.

In cases where there is not an adequate level of protection, the data transfer may take place when the data controllers in Turkey and in the relevant third country undertake, in writing, to provide adequate protection in the third country, as well as agree on the fact that the transfer is permitted by the Board of the KVKK.

The grounds for a cross-border **transfer includes the transfer being made from a register** which, according to the Union or a Member States' law, is intended to provide information to the public, and which is open to consultation either by the public in general or by any person who can demonstrate a **legitimate interest**, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Without prejudice to the provisions of international agreements, personal data can be transferred overseas **only by having regard to the opinion of the relevant state institutions** and organisations, in cases where the **interests of Turkey or the data subject may be seriously harmed**.

4.2. Data processing records

While the GDPR expressly requires data controllers and data processors to maintain a record of the processing activities under their responsibility, the LPPD does not establish such an obligation for either data controllers or data processors.

However, it should be noted that the LPPD includes a provision requiring data controllers to enrol in the VERBIS, providing, in their application, information similar to that which data controllers are required to include in their records of processing activities under the GDPR. VERBIS is principally kept and maintained by the KVKK, and is fundamentally different to records kept by controllers and processors.

GDPR Article 30 Recital 82	LPPD Article 16 Regulation on the Data Controller Registry 2017 ('the Regulation')

Similarities

Not applicable.	Not applicable.

Differences

Data controllers and data processors have an obligation to **maintain a record** of processing activities under their responsibility.	The LPPD provides that natural and legal persons **should enrol with VERBIS** before initiating processing. VERBIS is kept and maintained by the KVKK. Data controllers are responsible for the information published in VERBIS being complete, accurate, up to date, and lawful.
The GDPR **prescribes a list of information that a data controller** must record: • the name and contact details of the **data controller**; • the **purposes of the processing**; • a description of the categories of **personal data**; • the categories of recipients to whom the personal data will be **disclosed**; • the **estimated period for erasure** of the categories of data; and • a general description of the technical and organisational **security measures** that have been adopted.	The LPPD prescribes that **the following information should be included in the notification** alongside the application to VERBIS: • the **identity and address** of the controller, or, if applicable, their representative; • the **purposes of the processing**; • the description of the **group or groups of data subjects** and the **categories of personal data** (a data inventory); • the **recipient or group of recipients** to whom the personal data may be transferred; • the **personal data which may be transferred** to third countries; • the measures taken to ensure the **security of personal data**; and • the **maximum duration of the processing** necessary for the purposes of the processing itself. The Regulation provides a **list of additional information that must be included in the notification** alongside the application to VERBIS, including maximum data retention periods, details of contact person, as well as identifying types of information that

Differences (cont'd)

	will be publicly available. Any change to any information provided through the notification alongside the application to VERBIS must be immediately reported to the KVKK.
The requirements around data processing records shall not apply to **an organisation with less than 250 employees**, unless the processing: • is likely to result in a risk to the rights and freedoms of data subjects; • is not occasional; or • includes special categories of data in Article 9(1) (e.g. religious beliefs, ethnic origin, etc.) or is personal data relating to criminal convictions and offences in Article 10.	The following categories of data controllers are **exempt from having to register with VERBİS**: • data controllers employing less than 50 employees and with an annual balance less than TRY 25 million (approx. €2.4 million) (unless the data controller's main business activity is processing special categories of personal data); • data controllers processing personal data through non-automatic means, provided the processing is part of a data filing system; • public notaries; • associations; • foundations; • unions; • political parties; • lawyers; • public accountants and sworn-in public accountants; • customs brokers and authorised customs brokers; and • mediators.
The processing on information recorded by a data controller shall be in **writing or electronic form**.	VERBIS registration should be made via **the VERBIS online portal**. (Note, the deadline to register to VERBIS has expired as of 31 December 2021).
The obligations in relation to data processing records are also imposed on the **representatives of data controllers**.	The obligations in relation to VERBIS are fulfilled by **representatives** on behalf of **data controllers located outside Turkey**.

4.3. Data processing impact assessment

The GDPR provides for specific circumstances under which a DPIA must be conducted, whereas the LPPD does not include any requirement to undertake a DPIA or any similar obligation to evaluate the risk of personal data processing.

GDPR	LPPD
Articles 35, 36 Recitals 75, 84, 89-93	Not applicable

Similarities

GDPR	LPPD
Not applicable.	Not applicable.

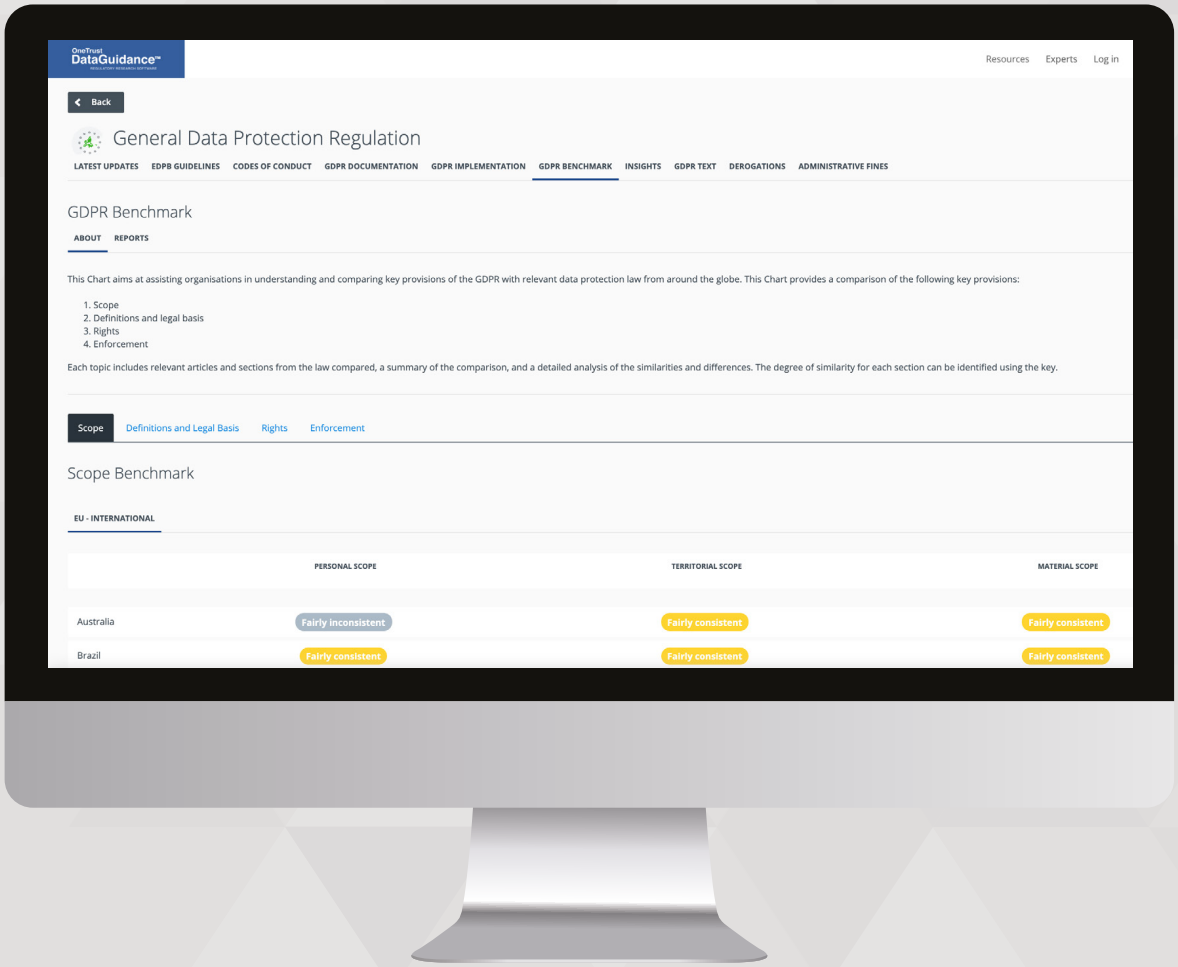
Differences

GDPR	LPPD
The GDPR provides that a DPIA must be conducted **under the following circumstances**: • if a data controller utilises **new technologies** to process personal data; • the processing may result in a high risk to the rights and freedoms of an individual; • when a systematic and extensive evaluation of personal aspects relating to natural persons is involved, which is based on automated processing or profiling; • there is processing on a large scale of special categories of data; and • there is systematic monitoring of a publicly accessible area on a large scale. In addition, the GDPR specifies requirements for **further reviews** and obligations for **prior consultation** with a supervisory authority. The GDPR also outlines that an assessment **must contain at least** the following: • a systematic description of the envisaged processing; • operations and legitimate purposes of the processing; • the necessity and proportionality of the • operations in relation to the purposes; and • the risks to the rights and freedoms of data subjects.	The LPPD does **not** establish DPIA obligations.

Global Regulatory Research Software

40 In-House Legal Researchers, 500 Lawyers Across 300 Jurisdictions

Monitor regulatory developments, mitigate risk, and achieve global compliance



OneTrust

DataGuidance™

REGULATORY RESEARCH SOFTWARE

Build a global privacy program by comparing key legal frameworks against the GDPR

CCPA | Russia | Thailand | Brazil | Japan | China
and 20+ other global laws & frameworks

Understand and compare key provisions of the GDPR with relivant data protection laws from around the globe

The GDPR Benchmarking tool provides comparison of the various pieces of legislation on the following key provisions


Scope


Rights


Definitions and legal basis


Enforcement

- Employ topic specific guidance to develop your compliance activities
- Monitor news and access written opinion pieces on the most recent developments

Start your free trial at

www.dataguidance.com

4.4. Data protection officer appointment

A major difference between the GDPR and the LPPD is that the GDPR provides that data controllers and data processors, including their representatives, must appoint a DPO, whereas the DPO concept is recently introduced to the LPPD, however there is no such requirement for appoint a DPO under the LPPD.

To provide a brief explanation, the Communiqué on the Procedures and Principles Regarding the Personnel Certification Mechanism introduced the concept of the DPO to Turkish law. As per the Communiqué on the Procedures and Principles Regarding the Personnel Certification Mechanism, a DPO is defined as a 'natural person who is entitled to use the title of data protection officer by successfully passing the exam', and it is stipulated that data protection officers have sufficient knowledge in terms of personal data protection legislation in addition to their certification program. However, unlike the GDPR, the Communiqué on the Procedures and Principles Regarding the Personnel Certification Mechanism does not regulate the concept of data protection officers in detail. The Communiqué on the Procedures and Principles Regarding the Personnel Certification Mechanism neither imposes any obligation on data controllers regarding the appointment of a data protection officer nor stipulates the duties of the DPO.

GDPR	LPPD
Articles 13-14, 37-39 Recital 97	Not applicable

Similarities

Not applicable.	Not applicable.

Differences

Under the GDPR, data controllers and data processors, including their representatives, are required to appoint a DPO. The GDPR also sets out numerous requirements related to DPOs, such as providing their contact details, ensuring they have adequate resources, and a wide range of DPO tasks and responsibilities.	There is no requirement for a data controller or their representative to appoint a DPO under the LPPD.

4.5. Data security and data breaches

Although only the GDPR includes integrity and confidentiality as explicit and fundamental principles of data protection, both the GDPR and the LPPD prescribe the adoption of technical measures to ensure the lawfulness of processing activities. In terms of data breach notification requirements, the GDPR and the LPPD provide a 72 hour timeframe to notify the competent supervisory authority.

However, while the GDPR contains specific exemptions to the obligation to notify of a data breach, the LPPD does not outline circumstances in which the notification to the Board of the KVKK and the data subject is exempted.

GDPR	LPPD
Article 5, 24, 32-34 Recitals 74-77, 83-88	Article 12 The Board Decision No. 2019/10 about Procedures and Principles of Personal Data Breach Notification ('the Decision') Guidance on Data Protection (technical and organisational measures)

Similarities

The GDPR recognises **integrity** and **confidentiality as fundamental principles** of protection by stating that personal data must be processed in a manner that ensures appropriate security of the personal data. The GDPR states that **data controllers and data processors are required to implement appropriate technical and organisational security measures** to ensure that the processing of personal data complies with the obligations of the GDPR.

The LPPD provides that the data controller is obliged to take any kind of **necessary technical and administrative measures** to ensure the appropriate level of security, with the purpose of:

- preventing unlawful processing of personal data;
- preventing unlawful access to personal data; and
- ensuring that personal data are safeguarded.

The data controller shall be **responsible** for taking the above measures, jointly with the data processor, in cases where personal data are processed by such natural or legal persons on their behalf.

In the case of a personal data breach, the **data controller must notify the competent supervisory authority** of a breach, unless the personal data breach is unlikely to **result in a risk** to the individuals' rights and freedoms.

In cases where the processed personal data are unlawfully collected by other persons, the data controller shall notify the same to the data subject and the Board of the KVKK within the **shortest time**. The Board of the KVKK may publicise the breach, when necessary, on its own website or by any other means that it deems appropriate.

Under the GDPR, a personal data breach must be notified to the supervisory authority **without undue delay** and, where feasible, **no later than 72 hours** after having become aware of the breach.

The Decision provides that the concept of 'shortest time' is interpreted as prescribing a period of **72 hours**. Therefore, the data controller must notify the Board of the KVKK without delay and not later than 72 hours after having become aware of the breach. The Decision further outlines that where the data breach notification cannot be made within 72 hours, the reasons for the delay should be attached to the notification to be made to the Board of the KVKK without undue further delay.

Similarities (cont'd)

The controller must **notify** the **data subject** of a data breach without undue delay if the data breach is likely to result in a **high risk** to the rights and freedoms of natural persons.

In addition, the Decision states that, from the date following the identification of persons affected by the data breach, **data subjects should be notified** about the breach in the shortest reasonable period of time. In particular, if the contact address of the data subject can be reached, notification should be made directly, or, in the case it cannot be reached, notification should be made by appropriate methods, such as the publication on the data controller's website.

The GDPR states that **data processors must notify** the data controller without **undue delay** after becoming aware of the personal data breach.

The Decision outlines that if personal data held by the **data processor** is obtained by others by unlawful methods, the data processor shall notify the data controller **without any delay**.

The GDPR **provides a list of information** that must be, at minimum, **included in the notification** of a personal data breach. For example, a notification must describe the nature of the breach, the approximate number of data subjects concerned, and the consequences of the breach.

In relation to the **information to be provided to the Board of the KVKK** when notifying the data breach, the Decision states that the controller must include the facts relating to the personal data breach, its effects, and the measures taken. The data controller shall be obliged to carry out necessary inspections, or have them carried out, in order to ensure that the provisions of the LPPD apply to their own institution or organisation.

The GDPR provides a **list** of **technical and organisational measures**, where appropriate, that data controllers and data processors must implement such as pseudonymisation, encryption and the ability to restore availability and access to personal data in a timely manner in the event of physical or technical incidents, to ensure integrity and confidentiality.

The Board of the KVKK, under its Guidance on Data Protection (technical and organisational measures) provides a **list** of **technical and organisational measures** to be taken by data processors, such as preparation of internal policies related to access, information security, retention and deletion of personal data, risk analyses, internal trainings, penetration test, network security, encryption etc.

Differences

Under the GDPR, the obligation of data controllers to notify data subjects when the data breach is likely to result in a high risk to the rights and freedoms of natural persons, **is exempted in certain circumstances** such as where:

- appropriate technical and organisational protective measures have been implemented;
- any subsequent measures have been taken in order to ensure that the risks are no longer likely to materialise; or
- it would involve is proportionate effort.

Under the LPPD, **there are no exemptions** to the obligation to notify unlawful collection of personal data to the Board of the KVKK and the data subject.

The GDPR does **not** explicitly require a data breach response plan.

The Decision further provides that, in case of a data breach, the data controller must prepare a **data breach response plan** to be reviewed periodically, including issues such as to whom the report will be provided by the controller, determination of who has the responsibility regarding the notification to be made under the LPPD, as well as the assessment of potential consequences of the data breach.

4.6. Accountability

Where the GDPR directly refers to the principle of accountability, the LPPD does not explicitly mention it. However, in the LPPD, a similar concept of controller responsibility can be inferred throughout provisions regarding the obligations of the data controllers and data processors.

GDPR	LPPD
Article 5, 24-25, 35, 37 Recital 39	Articles 3, 10, 12, 13, 16

Similarities

The GDPR recognises **accountability** as a fundamental principle of data protection. Article 5 states that 'the data controller shall be responsible and able to demonstrate compliance with, paragraph 1 [accountability].' In addition, the principles can be taken to apply to several other principles as mentioned in other sections of this report, including the appointment of a DPO, and DPIAs.

The LPPD does not explicitly refer to the principle of accountability. However, the LPPD **implies a similar level of responsibility** for the data controller and sets out various relevant obligations regarding, for example, data security, the application to VERBIS, responding to data subject requests, and providing the data subject with necessary information on the processing of their data. In addition, Article 12 states that: 'The controller shall be obliged to take any kind of necessary technical and administrative measures to ensure the appropriate level of security with the aim of: a) preventing unlawful processing of personal data; b) preventing unlawful access to personal data; c) ensuring that personal data are safeguarded.'

Differences

Not applicable.

Not applicable.

5. Individuals' rights

5.1. Right to erasure

The GDPR and the LPPD provide data subjects with the right to erasure of their personal data, where specific conditions are met, such as the purposes for processing no longer exist, or the data subject withdraws their consent. Unlike the GDPR, the LPPD does not explicitly provide exceptions to the right to erasure.

GDPR	LPPD
Articles 12, 17 Recitals 59, 65-66	Articles 7, 10, 11, 13 Article 12 of the Regulation on Erasure, Destruction or Anonymization of Personal Data

Similarities

The right to erasure applies to specific grounds, such as where **consent of the data subject is withdrawn** and there is with **no other legal ground** for processing, or the personal data **is no longer necessary** for the purpose of which it was collected.	Under the LPPD, personal data shall be erased by the controller, *ex officio* or upon demand by the data subject, if the reasons for processing **no longer exist**. Nevertheless, in any event, data subjects are entitled to request erasure of their personal data by applying to the data controller.
The right can be exercised **free of charge**. There may be some instances, however, where a fee may be requested, notably when requests are unfounded, excessive, or have a repetitive character.	The right can be exercised **free of charge**. However, data controllers may impose a fee on the applicant, as set by the KVKK, if the request necessitates a response.
A request can be made in **writing, orally, and through other means including electronic means** where appropriate.	A request can be made via **written or registered e-mail address, a secure electronic signature, a mobile signature or an e-mail** which is stated by data subjects or registered in the system of the data controller before the transaction, or an application/software prepared for the request.
Data subject requests under this right must be replied to without 'undue delay and in any event within **one month** from the receipt of request.' The deadline can be extended by **two additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request.	The data controller is obliged to process the data subject's enquiry and to take all necessary administrative and technical measures effectively in the shortest time possible or within **30 days** in accordance with the rule of law and good faith. This said, the LPPD **does not provide an extension period**.
Data subjects **must be informed** that they have the right to request for their data to be deleted, and are entitled to ask for their data to be erased.	As per the LPPD, data subjects **must be informed** that they have the right to request for their data to be deleted, and are entitled to ask for their data to be erased.

GDPR	LPPD

Similarities (Cont'd)

GDPR	LPPD
If the data controller has made personal data public and is obliged to erase the personal data, the data controller, taking into account the available technology and the cost of implementation, shall take reasonable steps, including **technical measures**, to **inform controllers** processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.	Following a data subject's request of erasure, if the conditions for the processing no longer exist and the personal data which are subject to the request have been transferred to any third party; the data controller is **obliged to notify** the third party that the data subject has requested the erasure and **shall ensure** that third parties duly conform with such request.
A data controller must have in place **mechanisms** to ensure that the request is made by the data subject whose personal data is to be deleted.	A data controller must have in place **mechanisms** to ensure that the request is made by the data subject whose personal data is to be deleted.

Differences

GDPR	LPPD
Exceptions to the right of erasure provided by the GDPR include: • **freedom of expression** and freedom of information; • complying with **public interest purposes in the area of public health**; • establishment, exercise, or defence of **legal claims**; and • **complying with legal obligations** for a public interest purpose.	The LPPD does **not** provide exceptions to the right of erasure.

5.2. Right to be informed

Both the GDPR and the LPPD recognise the right to be informed and impose an obligation to inform individuals of specific information relating to the 'processing' of personal data/information.

Unlike the GDPR, the LPPD does not make a distinction between sources of data when determining the content of the notification obligation and does not address the right of data subjects to be informed regarding the existence of automated decision-making and profiling.

GDPR Articles 5-14 Recitals 58 - 63	LPPD Articles 10, 11

Similarities

Data subjects must be provided with information relating to the processing of personal data in order to validate their consent, including:

- **details of personal data** to be processed;
- **purposes** of processing, including the legal basis for processing;
- **data subjects' rights** (e.g. the right to erasure, right to object, right of withdrawal, right to lodge a complaint to a relevant authority, etc.);
- **data retention period**;
- **recipients or their categories** of personal data; and
- **contact details** of the data controller or its representative and the DPO.

Data controllers must notify data subjects of the following as per Article 10 the LPPD:

- the **identity of the data controller** and of its representative, if any;
- the **purposes of the processing**;
- the **recipients** to whom the data can be transferred, and purposes of the transfer;
- the **method** and **legal ground** of the data collection; and
- the rights of data subjects as listed in Article 11.

Information can be provided to data subjects in an easily accessible form with clear and plain language, which can be in **writing and other means such as electronic format**.

Data controllers should inform data subjects in an 'understandable, clear and simple/plain' language, and should not use 'incomplete, misleading or false' information. There is **no specific form requirement** for notices (data subjects may be **orally** notified), however, the **burden of proof** lies with the data controller. Thus, data controllers tend to prefer to communicate notices in **writing**.

A data controller cannot collect and process personal data for purposes other than the ones about which the data subjects were informed, **unless the data controller provides them with further information**.

A data controller cannot collect and process personal data for purposes other than the ones about which the data subjects were informed, **unless the data controller provides them with further information**.

In the case of indirect collection, a data controller must provide information relating to such collection to data

In terms of personal data not obtained from the data subject, the LPPD requires that data controllers provide

GDPR	LPPD

Similarities (Cont'd)

subjects within a reasonable period after obtaining the data, but at the latest within one month, or **at the time of the first communication with the data subject, or when personal data is first disclosed to the recipient**.	the necessary information within a '**reasonable period**' similar to the GDPR. However, the LPPD provides for no specific deadline for fulfilling such obligation.
In case of direct collection, Information relating to personal data processing (e.g. the purpose of the processing, the rights of data subjects, etc.) must be provided to data subjects by the data controller **at the time when personal data is obtained**.	In case of direct collection, the information must be provided **when personal data is obtained**, at the latest.

Differences

The GDPR provides specific information that must be given to data subjects when their personal data has been **collected from a third party**, which includes the sources from which the data was collected.	The LPPD does **not** make a distinction between sources of the data, when determining the content of the notification obligation.
Data subjects must be informed of the existence of **automated decision-making, including profiling**, at the time when personal data is obtained.	The LPPD establishes a general requirement to provide information on methods of collection, but does **not** specifically refer to automated decision-making or profiling.
The GDPR **provides examples** of circumstances, which can be considered as 'legitimate interest.'	The LPPD **does not** specifically provide examples of circumstances that can be considered as 'legitimate interest.' However, in practice, the KVKK guidelines and decisions shed light on implementation of such a rule.
In addition, data subjects must be informed of the **possible consequences** of a failure to provide personal data whether in complying with statutory or contractual requirements, or a requirement necessary to enter into a contract.	The LPPD does **not** contain equivalent provisions.
A data controller must **inform** data subjects of the existence or absence of an adequacy decision, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference the **appropriate or suitable safeguards** and the means by which to obtain a copy of them or where they have been made available.	The LPPD does **not** contain a direct equivalent to this requirement but, to avoid liability for disclosure of personal information outside of Turkey, a data controller has to obtain explicit consent of the data subject to send their personal data to a recipient in a 'non-adequate' country.

5.3. Right to object


Fairly consistent

The GDPR provides data subjects with the right to object to the processing of personal data, as well as the right to withdraw consent to the processing of personal data. The LPPD also provides data subjects with the right to object to the processing of personal data, although it sets out a more limited scope for this right.

GDPR Articles 7, 18, 21	LPPD Articles 23, 27, 30

Similarities

Data subjects shall have the right to **withdraw** their consent to the processing of their personal data **at any time**.	The LPPD does not explicitly provide individuals with a right to withdraw their consent to the processing of their personal information at any time. However, by interpretation of its provisions, it is clear that data subjects shall have the right to **withdraw** their consent to the processing of their personal data **at any time**.
The data subject has the right to be **informed** about the right to object.	The data subject has the right to be **informed** about the right to object.
Data subjects must be provided with information about **how to exercise** this right.	Data subjects must be provided with information about **how to exercise** the right.
A request to restrict the processing of personal data must be responded to without undue delay and in any event within **one month** from the receipt of request. The deadline can be extended by **two additional months** taking into account the complexity and number of requests.	The data controller is obliged to process the data subject's enquiry and to take all necessary administrative and technical measures effectively in the shortest time possible or within **30 days** in accordance with the rule of law and good faith. This said, the LPPD **does not provide an extension period**.

Differences

Under the GDPR, data subjects are provided with the right to object to the processing of their personal data in specific circumstances: • the processing of personal data is due to **tasks carried out in the public interest** or **based on a legitimate interest pursued by the data controller** or **third party**; • the processing of personal data is for **direct marketing purposes**; and • the processing of personal data is for **scientific, historical research or statistical purposes**.	Under the LPPD, data subjects are provided with the right to object if they incur a result against them due to analyses of their data by **automatic means**.

GDPR	LPPD

Differences (cont'd)

Upon the receipt of an objection request, a data controller shall no longer process the personal data unless:

- **the processing is based on a legitimate ground** that overrides the data subjects' interests; or
- **it is for the establishment, exercise, or defence of a legal claim**.

The LPPD does **not** specifically regulate the conditions under which the data controller can reject a data subject's objection. Nevertheless, a data controller may refuse a data subject's request with justified grounds. However, the LPPD does not explicitly define 'justified grounds'.

5.4. Right of access

Both the GDPR and the LPPD provide individuals with the right to access their personal data when it is held or processed by a data controller. The LPPD, though, differs in its details on the format and content of the response.

GDPR	LPPD
Article 15 Recitals 59-64	Article 11

Similarities

The GDPR recognises that data subjects have the **right to access** their personal data that is processed by a data controller.

The LPPD recognises that data subjects have the right to **learn whether or not the personal data relating to themselves is being processed and if it is processed, request information with regard to the processing**. In addition, as per the Turkish Constitution, everyone has the constitutional right to access, delete, and/or correct the data processed about them.

The GDPR specifies that, **when responding to an access request**, the data controller must indicate the following information:

- the **purposes** of the processing;
- the **categories** of personal data concerned;
- the recipients or categories of recipients to whom the personal data has been or will be **disclosed**, in particular recipients in third countries or international organisations;
- where possible, the envisaged **period** for which the personal data will be **stored**, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller **rectification or erasure** of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a **complaint** with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their **source**; and
- the existence of **automated decision-making**, including profiling.

In general, data controllers must indicate the following information, when responding to a data subject's application to exercise their rights under Article 11 of LPPD:

- information related to the data controller or its representative;
- name, ID number (if applicant is a Turkish citizen), nationality, passport number or ID number (if applicant is a foreigner);
- notification address, e-mail address if any, phone and fax number of the applicant;
- **subject of the request**; and
- the data controller's **explanations** regarding the request.

Data subjects' requests under this right must be replied to without 'undue delay and in any event within one month from the receipt of a request.' The deadline can be extended by **two additional months** taking into account the complexity and number of requests. In any case,

The data controller is obliged to process the data subject's enquiry and to take all necessary administrative and technical measures effectively in the shortest time possible or within **30 days** in accordance with the rule of law and good faith. This said, the LPPD **does not provide an extension period**.

GDPR	LPPD

Similarities (cont'd)

the data subject must be informed of such an extension within one month from the receipt of a request.	
The right to access can be exercised **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive, or have a repetitive character.	The right can be exercised **free of charge**. However, the data controller may impose a fee on the applicant, as set by the KVKK, if the request necessitates a responding fee.

Differences

The GDPR provides that the right of access **must not adversely affect the rights or freedoms of others**.	The LPPD does not specifically draw a line for the exercise of the right to access. However, the KVKK ruled in one of its decisions (Decision Number 2020/13) that the exercise of a data subject's right to access should be '**reasonable**' and should not overstep the boundaries of a **data controller's technical fitness**.
A data controller can refuse to act on a request when it is **manifestly unfounded, excessive, or has a repetitive character**. The GDPR provides that the right of access must not adversely affect the rights or freedoms of others, **including those related to trade secrets**.	A data controller may refuse a data subject's request with **justified grounds**. However, the LPPD does **not** explicitly define 'justified grounds'. If the request is refused, the response of the controller is found unsatisfactory or the response is not given by the controller within 30 days, the data subject may file a complaint before the KVKK.
Data subjects must have a variety of means through which they can make their request, including **orally and through electronic means**. In addition, when a request is made through electronic means, a data controller should submit a response through the same means.	Data subjects can make their request via **written or registered e-mail address, a secure electronic signature, a mobile signature or an e-mail** which is stated by data subjects or registered in the system of a data controller before the transaction, or an application/software prepared for the application. The LPPD does **not** specify that the data controller should submit its response through the same means.
The GDPR specifies that a data controller must **have in place mechanisms** for identity verification.	The LPPD does **not** explicitly refer to equivalent identity verification mechanisms, however it does require that unlawful access is prevented.

5.5. Right not to be subject to discrimination

Neither the GDPR nor LPPD explicitly address the right not to be subject to discrimination. In both cases, however, it may be considered to be implied.

GDPR	LPPD

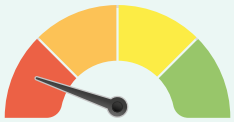
Similarities

GDPR	LPPD
The GDPR **does not** explicitly address the right not to be subject to discrimination; therefore, no scope of implementation is defined.	The LPPD **does not** explicitly address the right not to be subject to discrimination; therefore, no scope of implementation is defined.

Differences

GDPR	LPPD
Not applicable.	Not applicable.

5.6. Right to data portability



Inconsistent

The GDPR provides data subjects with the right to data portability, whereas the LPPD does not contain an equivalent right.

GDPR	LPPD
Articles 12, 20, 28 Recital 68, 73	Not applicable

Similarities

Not applicable.	Not applicable.

Differences

The GDPR provides individuals with the **right to data portability** and defines the right to data portability as the **right to receive data processed on the basis of contract or consent and processed by automated means, in a 'structured, commonly used, and machine-readable format'** and to transmit that data to another controller without hindrance.	The LPPD does **not** include a right to data portability.

6. Enforcement

6.1. Monetary penalties

Both the GDPR and the LPPD provide for monetary penalties to be issued in cases of non-compliance, although the amounts for such penalties differ significantly.

The main difference between the two laws is that the LPPD imposes both criminal and non-criminal penalties, whereas the GDPR only outlines administrative penalties for non-compliance.

GDPR	LPPD
Article 83-84 Recitals 148-149	Articles 17, 18

Similarities

GDPR	LPPD
The GDPR provides for the possibility of **administrative, monetary penalties** to be issued by the supervisory authorities in cases of non-compliance.	The LPPD provides for the possibility of **administrative, monetary penalties** to be issued by the supervisory authorities in cases of non-compliance. By reference to the Turkish Criminal Code, non-compliance with data protection rules under the LPPD could lead to criminal sanctions.

Differences

GDPR	LPPD
When applying an administrative sanction, the supervisory authority must consider: (i) the nature, gravity and duration of the infringement; (ii) the intentional or negligent character of the infringement; (iii) any action taken to mitigate the damage; (iv) the degree of responsibility of the controller or processor; (v) any relevant previous infringements; (vi) the degree of cooperation with the supervisory authority; (vii) the categories of personal data affected by the infringement; (viii) the manner in which the infringement became known to the supervisory authority; (ix) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures; (x) adherence to approved codes of conduct or approved certification mechanisms; and (xi) any other aggravating or mitigating factor applicable to the circumstances of the case.	The LPPD does **not** explicitly outline the criteria the Board of the KVKK must consider when applying an administrative sanction.
Supervisory authorities may **develop guidelines that establish further criteria** to calculate the amount of the monetary penalty.	The LPPD does **not** establish a similar provision.

GDPR	LPPD

Differences (cont'd)

The GDPR provides for the application of **fines to public bodies**. It is, though, left to Member States to create rules on the application of administrative fines to public authorities and bodies.	Under the LPPD, **government agencies cannot be sanctioned with administrative fines**. When the LPPD is violated by a governmental body, the KVKK will notify relevant institutions in order to conduct **disciplinary investigations against civil servants** who violate the prescribed obligations regarding the protection of personal data.
Depending on the violation occurred the penalty may be up to either: **2% of global annual turnover or €10 million**, whichever is higher; or **4% of global annual turnover or €20 million**, whichever is higher.	Administrative fines ranging between **TRY 13,400 (approx. €630**) and **TRY 2,680,000 (approx. €125,300)** will apply for breaches of the LPPD.
Under the GDPR, **it is left to Member States** to create rules on the application of administrative fines to public authorities and bodies.	Under the LPPD, government agencies **cannot** be sanctioned with administrative fines.

6.2. Supervisory authorities

Fairly consistent

Both the GDPR and the LPPD provide supervisory authorities with investigatory and corrective powers. However, there are some differences in the scope of such powers under each law.

GDPR	LPPD
Articles 51-84 Recitals 117-140	Articles 14, 15, 16, 18

Similarities

Under the GDPR, supervisory authorities have **investigatory powers** which include: (i) ordering a controller and processor to provide information required; (ii) conducting data protection audits; (iii) carrying out a review of certifications issued; and (iv) obtaining access to all personal data and to any premises.

Under the LPPD, supervisory authorities have **investigatory powers** which include: (i) ordering a controller and processor to provide required information; (ii) conducting data protection audits upon complaint or *ex officio*.

Under the GDPR, supervisory authorities have **corrective powers** which include: (i) issuing warnings and reprimands; (ii) imposing a temporary or definitive limitation including a ban on processing; (iii) ordering the rectification or erasure of personal data; and (iv) imposing administrative fines.

Under the LPPD, supervisory authorities have **corrective powers** which include: (i) ordering detected non-compliances to be remedied; (ii) ordering the processing or transfer of data abroad to be stopped; (iii) ordering the rectification or erasure of personal data; and (iv) imposing administrative fines. In addition, the KVKK is authorised to ensure that the VERBIS is maintained and, in cases of necessity, to make exceptions to the obligation to register with VERBIS.

Under the GDPR, supervisory authorities shall also: (i) **handle complaints** lodged by data subjects; and (ii) **cooperate with data protection authorities** from other countries.

Under the LPPD, supervisory authorities shall also: (i) **handle complaints** lodged by data subjects; and (ii) **cooperate** with other governmental bodies, non-governmental organisations, professional associations and universities when data protection related issues are concerned.

Under the GDPR, supervisory authorities are tasked with **promoting public awareness** and understanding of the risks, rules, safeguards and rights in relation to processing as well as promoting the awareness of controllers and processors of their obligations, amongst other tasks.

Under the secondary legislation of the LPPD, supervisory authorities are tasked with **promoting public awareness** in relation to protection of personal data.

Differences

Supervisory authorities may be subject to financial control only if it does not affect its **independence**.

The LPPD does **not** include specific provisions on supervision of supervisory authorities. This said, as per general rules of

GDPR	LPPD

Differences (Cont'd)

They have separate, public annual budgets, which may be part of the overall national budget.	Turkish laws, supervisory authorities **may be subject to financial control**. Supervisory authorities have separate, public annual budgets, which may be part of the overall national budget.
It is **left to each Member State** to establish a supervisory authority, and to determine the qualifications required to be a member, and the obligations related to the work, such as duration of term as well as conditions for reappointment.	The LPPD does **not** contain equivalent provisions.

Fairly consistent

6.3. Civil remedies for individuals

Both the LPPD and the GDPR provide the right for a data subject to lodge a complaint with the supervisory authority. Similar to the GDPR, Turkish laws provide data subjects with a lawful right to claim for compensation for any damages incurred due to data protection violations.

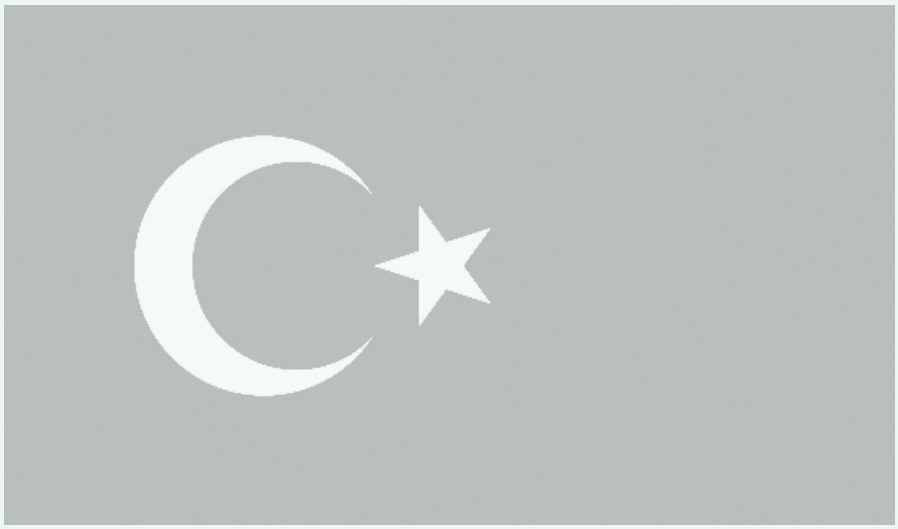
GDPR	LPPD
Articles 79, 80, 82 Recitals 131, 146-147, 149	Article 14

Similarities

GDPR	LPPD
The GDPR provides individuals with a cause of action to **seek compensation** from a data controller and data processor for a violation of the GDPR.	Individuals can claim **compensation** for unlawful collection or processing of personal data accordingly with the **Turkish Civil Code**.
Under the GDPR, the data subject has the right to **lodge a complaint** with the supervisory authority. The supervisory authority must inform the data subject of the progress and outcome of their complaint.	Under the LPPD, the data subject has the right to **lodge a complaint** with the KVKK. The KVKK must inform the data subject of the progress and outcome of their complaint.

Differences

GDPR	LPPD
The GDPR provides that a data controller or processor shall be **exempt from liability to provide compensation** if it proves that it is not in any way responsible for the event giving rise to the damage.	The LPPD does **not** explicitly provide such exemptions.
The GDPR allows Member States to provide for the possibility for data subjects to give a mandate for representation to a **not-for-profit body, association, or organisation** that has as its statutory objective the protection of data subject rights.	The LPPD does **not** address this issue.



Our Information Technology & Communications practice

We have an acute understanding and knowledge of the industry that is invaluable to our clients who seek to remain innovative and profitable within this rapidly developing sector.

The continuous evolution of Information Technology & Communications markets creates both opportunities for designing new and profitable ways of sourcing IT/C products and services and legal risks. Our team of professionals utilizes their long-standing expertise of both the technical and legal aspects of Information Technology & Communications to help our clients navigate the sector's complex legal and commercial risks.

We help clients with:

- Telecommunications
- New and mainstream media
- Clouds
- E-commerce
- Fintech
- Artificial Intelligence
- E-notification
- E-signature
- IT/C & Regulatory in M&A deals
- IT Outsourcing
- Privacy & Data Protection
- IT/C related agreements
- IT/C related administrative and civil litigation
- Blockchain

Directory rankings & quotes:

Tier 1 – Media & Entertainment

Tier 2 - IT and Telecoms

Band 2: TMT

"Experience and extensive knowledge."

Chambers Europe, 2020

"They have a very welcoming approach and they do their best to support you."

Chambers Europe, 2020

"Starting from the first correspondence phase Esin Attorney Partnership is always very professional."

Legal 500, 2020

"They have a big team and every sub-group is experienced in different areas; you are always consulting with a senior lawyer."

Legal 500, 2020

"Team members are practical and easy to work with."

Legal 500, 2020

"They have provided us with excellent information in such short time periods regarding compliance to data privacy regulations"

Legal 500, 2020

Key Contacts:

İlay Yılmaz
Partner | CIPP/E
T: +90 549 812 0558
ilay.yilmaz@esin.av.tr

Can Sözer
Senior Associate
T: +90 530 555 3963
can.sozer@esin.av.tr

Esin
Attorney
Partnership.

Esin Attorney Partnership helps clients overcome the challenges of competing in the global economy.

esin.av.tr