

Personal Data Protection Guide

(KVKK) Practical Information and Best Practices



Introduction

Personal data has become one of the key elements shaping a wide range of areas, from individuals' identities to their behaviours, in today's increasingly digital world. This guide has been prepared to present, in a clear and accessible manner, the fundamental concepts, obligations, and legal remedies related to the protection of personal data in Turkey, under Law No. 6698 on the Protection of Personal Data ("KVKK"), to both organisations and data subjects.

The main purpose of this guide is to raise awareness among data controllers and data processors regarding the rules they must follow and the obligations they must meet when processing personal data. It also aims to inform individuals whose personal data is processed of their rights under the KVKK and to serve as a practical reference for real-life applications.

This guide is intended not only for legal professionals but also for all natural and legal persons involved in data processing, including public institutions, private sector organisations, and individuals.

The guide covers topics such as:

- Conditions for processing personal data
- Explicit consent and the obligation to inform
- Transfer of data abroad
- Technical and administrative measures required for data security
- The obligation to register with VERBIS and exemptions
- Rights of data subjects and means of recourse

All these topics are explained in plain language and supported by example decisions and implementation guidelines from the Personal Data Protection Authority.

For institutions, this guide provides a resource for launching or updating their KVKK compliance processes. For individuals, it offers a valuable tool for understanding and asserting their rights over their personal data.

Definitions

Explicit Consent: Consent that relates to a specific subject, is based on informed understanding, and is given freely.

Occasional Transfer: A data transfer that is irregular, occurs once or only a few times, is not continuous, and does not take place in the ordinary course of business.

Personal Data: Any information relating to an identified or identifiable natural person.

Processing of Personal Data: Any operation performed on personal data by wholly or partly automated means, or, if not automated, as part of a data recording system. This includes collection, recording, storage, preservation, alteration, rearrangement, disclosure, transfer, acquisition, making available, classification, or prevention of use.

Anonymisation: Rendering personal data impossible to associate with an identified or identifiable natural person, even when matched with other data.

Binding Corporate Rules: Internal rules that form one legal basis for transferring personal data abroad and must be followed by companies within the same corporate group.

EDPB (*European Data Protection Board*): The EU body responsible for ensuring consistent application of the GDPR across Member States.

GDPR (*General Data Protection Regulation*): The General Data Protection Regulation of the European Union.

Board: The Personal Data Protection Board.

Authority: The Personal Data Protection Authority.

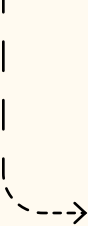
Special Categories of Personal Data: Data relating to a person's race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and attire, membership in associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.

Data Subject: The natural person whose personal data is processed.

Data Processor: A natural or legal person who processes personal data on behalf of the data controller, under the authority granted by the controller.

Data Controller: A natural or legal person who determines the purposes and means of processing personal data, and who is responsible for establishing and managing the data recording system.

Table of Contents



06	Fundamental Principles and Conditions for Processing Personal Data • Fundamental Principles • Conditions for Processing Special Categories of Personal Data • Explicit Consent of the Data Subject • Data Controller and Data Processor
14	Obligations of the Data Controller • Obligation to Inform the Data Subject • VERBIS – Obligation to Register with the Data Controllers’ Registry • Technical and Administrative Measures for Data Security
19	Transfer of Personal Data Abroad • Adequacy Decision • Appropriate Safeguards • Exceptional Transfers of Personal Data Abroad
24	Rights of Data Subjects and Remedies

Fundamental Principles **and** **Conditions for Processing Personal Data**

Conditions for Processing Personal Data

Conditions for Processing Special Categories of Personal Data

Explicit Consent of the Data Subject

Data Controller and Data Processor



Fundamental Principles and Conditions for Processing Personal Data

Fundamental Principles

According to Article 4 of the KVKK, personal data processing activities must comply with the following fundamental principles:

- **Compliance with the law and the rules of honesty:**
Personal data must be processed in accordance with applicable laws and regulations. The process should be transparent to the data subject and aligned with the stated purpose.
- **Being accurate and, where necessary, kept up to date:**
The accuracy of the sources from which personal data is collected must be verified, and any requests from data subjects to correct their personal data must be honoured.
- **Processed for specified, explicit and legitimate purposes:**
The legal basis and purpose of processing must be specific, clear, and transparent to the data subject. Personal data must not be used for purposes beyond those explicitly stated.
- **Relevant, limited and proportionate to the purpose:**
In line with the “data minimisation” principle under the GDPR, only data necessary for the stated purpose should be processed. Any data that is irrelevant or excessive must not be collected or used.
- **Stored for the period required for the purpose:**
As an extension of the purpose limitation principle, personal data must not be retained longer than is necessary for the purpose of processing.

Decision of the Board dated 3 August 2023 and numbered 2023/1327:

Regarding the sharing of a data subject’s personal data by hotel staff with third parties:

Housekeeping staff are responsible primarily for cleaning and maintenance services, which do not require access to the guest’s name or surname. In seeking to make guests feel special, the data controller must not disregard the right to personal data protection and should offer individuals the right to choose. In line with the data minimisation principle, including guests’ names and surnames on the “Housekeeping Task Sheet” was deemed a disproportionate processing activity under Article 4 of the Law.

Decision of the Board dated 2 May 2023 and numbered 2023/692:

A private healthcare institution acting as the data controller did not allow the appointment booking process to proceed unless the data subject provided explicit consent to the processing of personal data. This requirement undermines the principle of “freely given” consent, a core aspect of valid explicit consent, and constitutes a breach of the principle of compliance with the law and rules of honesty under Article 4 of the Law.

Conditions for Processing Personal Data

Personal data may only be processed if at least one of the legal grounds listed in Article 5 of the KVKK is present.

- ***The data subject's explicit consent to the processing activity***

Before initiating any data processing, the data controller must first determine whether a valid legal basis exists. Explicit consent should only be relied upon if no other legal ground applies. Where another legal basis is available, the controller must not seek consent.

The data subject must always have the right to withdraw their explicit consent. If processing is based on consent but continues after withdrawal by switching to another legal ground, this breaches the principles of lawfulness and fairness. Further detail is provided in the section "*Explicit Consent of the Data Subject.*"

It is important to note that the existence of explicit consent alone does not automatically render a processing activity lawful under the KVKK.

- ***Processing is explicitly provided for by law***

Where a legal obligation expressly requires personal data to be processed, this constitutes a valid legal basis.

For example, under Article 75 of the Labour Law No. 4857, employers must maintain a personnel file for each employee, including identification details and other documents required by law. The processing of this data is therefore legally mandated.

- ***Processing is necessary to protect the life or physical integrity of the data subject or another person who is unable to give consent due to actual impossibility or whose consent is not legally valid***

According to the *Guide on Conditions for Processing Personal Data*, data on a phone found with a person deprived of liberty may be processed to help locate them under this exception.

Similarly, Recital 46 of the GDPR notes that this ground may apply in situations involving public health emergencies, such as epidemics or natural disasters

- ***Processing is necessary for the establishment or performance of a contract***

Where the processing of personal data is essential to enter into or perform a contract with the data subject, it is lawful.

For example, in a sales contract, the seller must process the buyer's address to deliver goods, and the buyer may process the seller's bank details to make payment.

- ***Processing is necessary for the data controller to fulfil a legal obligation***

If the data controller is subject to regulatory obligations requiring certain data to be processed, this ground applies.

For instance, banks may process customer and transaction data to meet legal retention requirements.

- ***The data subject has made the personal data public***

Where an individual voluntarily makes their personal data public, it may be processed, but only for purposes consistent with the original disclosure.

For example, if someone includes their contact details in a car sale advertisement, those details may only be used in relation to that advert.

- ***Processing is necessary for the establishment, exercise or defence of a legal right***

Personal data that may serve as evidence in legal proceedings can be retained during the applicable statute of limitations period under this legal ground.

- ***Processing is necessary for the legitimate interests of the data controller, provided that it does not infringe the fundamental rights and freedoms of the data subject***

The Guide on Conditions for Processing Personal Data clarifies that the interest must be legitimate, specific, concrete, effective, and present. It must also be balanced against the data subject's fundamental rights.

For instance, an employer may process personal data related to employee performance in connection with a bonus or incentive system designed to improve engagement.

Special Categories of Personal Data

Special categories of personal data are considered more sensitive than other types, as their processing could lead to discrimination or otherwise harm the data subject. For this reason, they are subject to stricter legal protections.

As a general rule, the processing of special categories of personal data is prohibited, unless one of the specific exceptions set out in the KVKK applies or the data subject has given explicit consent.

The KVKK defines which types of data fall under this category and sets out the conditions under which they may be lawfully processed.

Special categories of personal data include:

- Race
- Ethnic origin
- Political opinions
- Philosophical beliefs
- Religion, sect, or other beliefs
- Appearance and attire
- Membership in associations, foundations, or trade unions
- Health
- Sexual life
- Criminal convictions and security measures
- Biometric data
- Genetic data

Conditions for Processing Special Categories of Personal Data

According to Article 6(3) of the KVKK, special categories of personal data may only be processed if at least one of the following conditions is met:

- *The data subject has given explicit consent.*
- *The processing is explicitly provided for by law.*
- *It is necessary to protect the life or physical integrity of the data subject or another person who is unable to give consent due to actual impossibility or whose consent is not legally valid.*
- *The personal data has been made public by the data subject, and the processing is in line with the intent of that disclosure.*
- *It is necessary for the establishment, exercise, or defence of a legal right.*
- *It is necessary for reasons of public health, preventive medicine, medical diagnosis, treatment or care services, or the planning, management, and financing of health services provided the processing is carried out by persons subject to a confidentiality obligation or by authorised institutions and organisations.*
- *It is necessary to fulfil obligations in the fields of employment, occupational health and safety, social security, social services, or social assistance.*
- *The processing is carried out by foundations, associations, or other non-profit organisations or formations established for political, philosophical, religious, or trade union purposes, in accordance with the relevant legislation and their legitimate purposes. The processing must be limited to their field of activity, must not be disclosed to third parties, and must relate only to their current or former members, affiliates, or regular contacts.*

Explicit Consent of the Data Subject

According to the KVKK, explicit consent must meet the following conditions:

- It must relate to a specific subject.
- It must be based on information.
- It must be freely given.

Under the European Union's General Data Protection Regulation (GDPR), explicit consent is defined as *"a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them."*

Balance of Power and Free Will

For consent to be considered *freely given*, there must be a balance of power between the data controller and the data subject. The KVKK's *Explicit Consent Guide* emphasises:

"In cases where the parties are not in an equal position or where one party has influence over the other, careful assessment is required whether the consent was truly given of the data subject's own free will."

Evaluating power dynamics is essential. Consent given due to fear of negative consequences or embedded

within a non-negotiable contract cannot be considered valid under the KVKK.

Typical examples of power imbalance include relationships where the data controller is an employer or public authority. In such cases, consent may not be considered voluntary.

The *Explicit Consent Guide* clearly states:

“Particularly in the employer-employee relationship, where the employee is not effectively given the option to withhold consent or where withholding consent would likely result in adverse consequences, consent cannot be deemed to be given of free will.”

This principle is also recognised by the European Data Protection Board (EDPB) in its *Guidelines 05/2020 on Consent*, adopted on 4 May 2020. It states that, due to the inherent power imbalance, it is difficult to consider

employee consent to be freely given. The risk of job loss makes it unlikely that an employee can genuinely object to data processing.

Similarly, the Article 29 Working Party, in its *Opinion 8/2001 on the Processing of Personal Data in the Employment Context* (13 September 2001), stressed that when employers need to process personal data as a necessary part of the employment relationship, relying on employee consent is misleading. Consent should only be sought when the employee has a real choice and can withdraw consent without facing any disadvantage.

For example, where employee data is processed for personnel files, payroll, or bank account details used for salary payments, it is more appropriate to rely on legal or contractual grounds than to seek explicit consent.

Decision of the Board dated 10 August 2023, No. 2023/1356:

On the submission of video footage showing a data subject praying in a mosque, used as evidence in a reinstatement case:

“It was determined from the email sent by a staff member of the data controller to the data subject that consent was not freely given. The data subject was compelled to retroactively sign documents concerning personal data processing due to fear of being dismissed from employment.”

Decision of the Board dated 8 July 2019, No. 2019/206:

“If the data processing activity is based on a legal ground other than explicit consent under the Law, there is no need to obtain explicit consent from the data subject. Relying on explicit consent despite the availability of another legal ground is considered deceptive and an abuse of rights.”

Decision of the Board dated 31 August 2023, No. 2023/1509:

“Personal data cannot be processed without the data subject’s explicit consent or another legal ground listed in Article 5(2) of the Law. If the processing is based on another legal ground, obtaining explicit consent would be misleading and is not required. In such cases, the absence or withdrawal of consent is legally irrelevant.”

The Relationship Between Explicit Consent and the Obligation to Inform

Obtaining explicit consent and fulfilling the obligation to inform are two distinct and independent requirements. They must not be carried out within the same process or document.

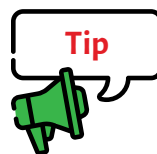
Requesting consent at the same time as providing the information notice may result in the data subject giving consent before having time to properly consider the information. It is essential to remember that the data subject may choose not to give consent after reading the notice.

Decision of the Board dated 26 July 2018, No. 2018/90:

“The purpose of fulfilling the obligation to inform is to ensure that the data subject is made aware of the processing of their personal data. The purpose of obtaining explicit consent is to provide a legal basis for the data controller to process personal data.

Therefore, although the data subject becomes informed about the processing by reading the information notice, they are not obliged to give consent to what is written in that notice.”

“There must be separate mechanisms to confirm that the data subject has read the information notice and to obtain proof of their approval of the explicit consent form, which must include appropriate opt-in options.”



→ Obtaining explicit consent and fulfilling the obligation to inform are separate legal processes. They must not be combined into a single procedure.

Data Controller and Data Processor

To ensure the security of personal data, it is essential to clearly define the roles of *data controller* and *data processor*. This distinction determines how responsibilities are allocated between parties involved in data processing, guides the drafting of appropriate legal documentation, and clarifies how data subjects may exercise their rights. Under the KVKK:

Data Processor: A natural or legal person who processes personal data on behalf of the data controller, based on the authority granted by the controller.

Data Controller: A natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.

According to the *Guide on Data Controllers and Data Processors*, the data controller is the party who determines the purpose and method of processing in other words, the one who can answer the questions: *why* is the data being processed, and *how* is it being processed? The guide also highlights several factors that must be considered when identifying the data controller:

The guide also highlights several factors that must be considered when identifying the data controller:

- Who decides on the collection of personal data and the method of collection?
- Which types of personal data are to be collected?
- For what purposes will the collected data be used?
- Whose personal data will be collected?
- Will the data be shared, and if so, with whom?
- How long will the data be retained?

To qualify as a data processor, a natural or legal person must be separate from the data controller and must process personal data solely on the controller's behalf. The same person or entity may act as a data processor in some cases and as a data controller in others, depending on the nature of the processing activity.

The data controller is the entity that determines the purposes and means of processing personal data.

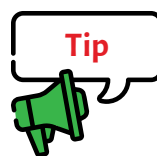
When identifying a data controller, it is important to ask: *To what extent does the party determine the purpose and method of data processing?* That degree of control is key to establishing whether the party qualifies as a controller.

While a data controller may delegate certain responsibilities to a data processor; particularly concerning administrative and technical measures for data security some decisions must always remain with the controller.

According to the *Guide on Data Controllers and Data Processors*, a data processor may be authorised to make decisions on:

- Which IT systems or other methods are used to collect personal data
- How personal data is stored
- The specific security measures to be implemented
- The method used to transfer personal data
- How retention periods are applied
- The procedures for deletion, destruction, or anonymisation of personal data

However, the authority to determine **which** data is processed, **how long** it is retained, and **who** has access to it must always rest with the data controller.



→ In a contract, simply labelling a party as a data controller or processor is not enough to determine their actual role. The factual circumstances of the processing activity must be assessed.

Obligations of the Data Controller

Obligation to Inform the Data Subject

VERBIS – Obligation to Register with the Data Controllers' Registry

Technical and Administrative Measures for Data Security



Obligations of the Data Controller

Obligation to Inform the Data Subject

When does the obligation to inform arise?

The obligation to inform applies in every instance where personal data is processed. The data controller must fulfil this obligation *before* processing the data subject's personal data.

If personal data that was previously processed for a specific purpose and under a specific legal ground is later to be used for a different purpose or legal basis, the data subject must be informed in advance of this new processing activity.

What must an information notice include?

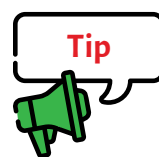
An information notice must include, at a minimum, the following:

- The identity of the data controller and, if applicable, their representative
- The purpose(s) for which the personal data will be processed
- The categories of recipients to whom the personal data may be disclosed, and the purposes of such disclosures
- The method and legal basis for collecting the personal data
- The rights of the data subject as set out in the Law

These are the *minimum* required elements. Additional detail should be provided where necessary. For example, when identifying the data controller or their representative, their contact information should also be included.

Decision of the Board dated 1 June 2023, No. 2023/938:

If students are to receive announcements via their institutional email addresses, this must be clearly disclosed in the information notice.



→ Avoid vague or overly general language in information notices. Terms such as “to provide better service” or “to develop new services” are too broad and do not meet the requirement of specificity under the KVKK.

Does approval of the information notice constitute explicit consent?

No. If the legal basis for processing is the data subject's *explicit consent*, then two distinct approvals must be obtained:

1. Confirmation that the information notice has been read and understood
2. The explicit consent itself

To prevent confusion, the confirmation that the notice has been read should not use phrases like “*I approve the information notice*” or “*I accept the information notice.*” A clearer alternative is: “*I have read and understood the information notice.*”

Decision of the Board dated 28 September 2023, No. 2023/1653:

Obtaining explicit consent through commercial electronic messages during a shopping transaction may give the false impression that consent is required to complete the transaction, undermining the requirement of free will.

In in-store shopping scenarios, the purpose of sending an SMS to the customer and the consequence of providing the received code must be explained clearly by authorised personnel as part of a layered information process. Therefore, the information notice and the explicit consent confirmation code must not be included in the same SMS message.

Who bears the burden of proof for fulfilling the obligation to inform?

The data controller bears the burden of proof. It is therefore advisable to provide the information notice in written form and request that the data subject confirm, also in writing, that they have read and understood it.

VERBIS - Obligation to Register with the Data Controllers' Registry

Under the KVKK and the Regulation on the Data Controllers' Registry, all data controllers; unless specifically exempt; are required to register with the **Data Controllers' Registry (VERBIS)** via the official online system before commencing any personal data processing activities.

Data controllers must complete their registration within 30 days from the date on which they become subject to the registration requirement. If, due to factual, technical, or legal obstacles, they are unable to meet this deadline, they must submit a written request for an extension to the Authority within 7 business days. The Authority may grant a one-time extension not exceeding 30 days.

The registration must include the following information:

- Identity and contact details of the data controller, its representative (*if applicable*), and its designated contact person
- The purposes for which personal data will be processed
- Categories of data subjects and types of personal data
- Recipients or recipient groups to whom personal data may be disclosed
- Personal data intended to be transferred abroad
- Security measures taken to protect personal data
- Retention periods for the processed personal data

If any of the recorded information changes, the data controller must update the registry via VERBIS within seven days of the change.

In addition to registration, data controllers subject to this obligation must also prepare a Personal Data Processing Inventory.

Exemptions from VERBIS Registration

The following categories of data controllers are exempt from the obligation to register with VERBIS:

- Those who process personal data only through non-automated means, provided the data forms part of a structured recording system
- Notaries
- Associations, foundations, and trade unions, provided they process personal data solely in line with applicable legislation and only in respect of their own employees, members, affiliates, and donors
- Political parties
- Lawyers
- Customs brokers
- Mediators
- Certified public accountants and sworn-in certified public accountants
- Natural or legal person data controllers with fewer than 50 employees and an annual financial balance below TRY 100 million, whose primary activity does not involve processing special categories of personal data
- Village legal entities

Technical and Administrative Measures for Data Security

Under the KVKK, data controllers are required to take all necessary technical and administrative measures to ensure the security of personal data.

Article 12 of the KVKK states:

The data controller shall:

- a) Prevent the unlawful processing of personal data
 - b) Prevent unlawful access to personal data
 - c) Ensure the secure storage of personal data
- by taking every necessary technical and administrative measure to establish an appropriate level of security.

To determine which measures are necessary, data controllers must understand their data processing activities in full and assess the specific risks of data breaches associated with each activity.

Decision of the Board dated 3 August 2023, No. 2023/1327:

On the disclosure of a guest's personal data by hotel staff:

The inclusion of personal data on the Housekeeping Task Sheet, which was subsequently accessed by third parties, occurred solely because the data controller failed to implement adequate administrative and technical safeguards.

Data security involves more than cyber protection. It must also include organisational and physical safeguards. In some cases, industry-specific legislation or regulator-issued guidance may impose additional obligations. These must also be observed.

"Everything is prohibited unless permitted."

The Personal Data Security Guide emphasises that the correct approach is not "everything is permitted unless prohibited" but rather "everything is prohibited unless explicitly permitted."

Establishing internal policies on personal data processing and protection is critical to building a culture of compliance and ensuring that employees understand and follow proper procedures.

Access to Personal Data

Access must be limited strictly to individuals who need the data to perform their duties. To prevent unauthorised internal access, it is recommended to implement an access control and authorisation matrix.

Decision of the Board dated 6 July 2023, No. 2023/1130:

On the unauthorised sharing of medical data with a data subject's former spouse:

The pharmacist, as data controller, failed to take adequate technical and administrative measures, as required by Article 12 of the Law. Despite being liable under Article 116 of the Turkish Code of Obligations for the actions of their employees, the pharmacist did not demonstrate due care in supervising or instructing staff, leading to the unlawful disclosure of sensitive health data.

Decision of the Board dated 24 August 2023, No. 2023/1465:

On the unauthorised viewing of user data via a car rental platform:

Due to an algorithm malfunction, users logging into the platform were able to access personal data belonging to others. This indicated a clear failure by the data controller to meet its data security obligations.

Data Breach Notification Obligation

Data controllers must notify the Board as soon as possible in the event of a personal data breach, particularly if data is unlawfully accessed or acquired by third parties.

Decision of the Board dated 1 June 2023, No. 2023/928:

A university sent documents containing personal data to third parties via email. Despite this being a data breach, the university failed to notify the Board, violating the notification obligation under Article 12.

Measures Concerning Data Processors

When appointing a data processor, the data controller must ensure that the processor has implemented adequate technical and administrative security measures in accordance with the KVKK. This obligation must be clearly stated in the data processing agreement.

The *Personal Data Security Guide* recommends that such agreements:

- Include a clause confirming that the data processor's confidentiality obligations continue indefinitely
- Reserve the data controller's right to audit the processor's systems, or to appoint a third party to carry out such audits

To effectively monitor data security, the Guide further recommends that data controllers:

- Control which software and services are active on information networks
- Detect intrusions into these networks
- Regularly record and review user activity logs
- Ensure prompt reporting of security incidents
- Establish formal procedures for employees to report system or service vulnerabilities

These measures ensure that the data processor remains compliant and that the data controller retains ultimate responsibility for maintaining data security.

Transfer of Personal Data Abroad

Adequacy Decision

Appropriate Safeguards

Exceptional Transfers of Personal Data Abroad



Transfer of Personal Data Abroad

The *Regulation on the Procedures and Principles for the Transfer of Personal Data Abroad* defines the transfer of personal data abroad as:

“The transmission of personal data by a data controller or data processor within the scope of Law No. 6698 to a data controller or data processor located abroad, or making the data accessible by other means.”

In addition to meeting one of the legal grounds for processing set out in the KVKK, personal data may only be transferred abroad if one of the following conditions is also met:

Adequacy Decision:

An adequacy decision must have been issued by the Board regarding the recipient country, a sector within that country, or an international organisation.

Appropriate Safeguards:

Where no adequacy decision exists, personal data may still be transferred abroad if one of the following safeguards is in place:

- i. An agreement between a **foreign public institution or organisation** and a **Turkish public institution or organisation**, with the Board's approval for the transfer
- ii. The existence of **Binding Corporate Rules (BCRs)** approved by the Board
- iii. A **Standard Contract** published by the Board
- iv. A **written undertaking** including adequate protection clauses, along with the Board's permission for the transfer

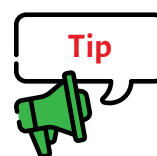
If **none** of these conditions is met, personal data may only be transferred abroad on an **exceptional and occasional basis**.

Adequacy Decision

If the Board has issued an adequacy decision regarding a particular country, sector, or international organisation, personal data may be transferred to that destination without requiring additional safeguards.

In evaluating whether to issue such a decision, the Board considers the following:

- i. Whether **reciprocity** exists in the transfer of personal data between Turkey and the relevant country, sector, or organisation
- ii. The **data protection legislation** and regulatory framework of the recipient
- iii. The presence of an **independent and effective data protection authority**, and the availability of administrative and judicial remedies
- iv. Whether the recipient is a party to international conventions or a member of international data protection organisations
- v. Whether the country or organisation is part of global or regional bodies to which Turkey also belongs
- vi. Whether there are **international agreements** to which Turkey is a party



→ As of the date this guide was published, the Board has not issued any adequacy decisions.

Appropriate Safeguards

If no adequacy decision has been issued by the Board, personal data may still be transferred abroad provided that appropriate safeguards are in place. These safeguards must be approved or recognised by the Board. Four types of safeguards are accepted:

1) *Non-international Agreements Between Public Institutions*

Appropriate safeguards may be established through agreements concluded between Turkish public institutions or organisations and foreign public institutions (*not constituting international treaties*).

To be valid, the agreement must include provisions covering:

- The purpose, scope, nature, and legal basis of the data transfer
- Definitions of key terms
- A commitment to comply with the fundamental principles set out in the KVKK
- Provisions for informing data subjects about the transfer
- Commitments related to the exercise of data subject rights under the KVKK
- Technical and administrative data security measures
- Measures for transferring special categories of personal data
- Restrictions on onward transfers
- Legal remedies available to data subjects
- Audit mechanisms
- Clauses granting the data exporter the right to suspend or terminate the agreement if the importer fails to comply
- A commitment by the data importer to return all personal data (including backups) or permanently destroy it upon termination or expiry of the agreement

2) *Binding Corporate Rules (BCRs)*

Companies within a corporate group engaged in joint economic activity may provide appropriate safeguards through Binding Corporate Rules.

- Transfers based on BCRs require prior approval from the Board.
- If BCRs are submitted in a foreign language, the Turkish version will be considered authoritative for the Board's decision.

The BCRs must include:

- Organisational structure and contact details of each group member
- Categories of personal data, purposes of processing, data subject groups, recipient countries, and transfer mechanisms
- A declaration that the BCRs are legally binding
- Compliance with the core principles of the KVKK
- Conditions for processing both ordinary and special categories of personal data
- Technical and administrative measures to ensure data security
- Restrictions on onward transfers
- Other applicable data protection safeguards
- A commitment to uphold data subject rights and permit complaints to the Board
- A declaration by a Turkey-based group entity accepting liability for violations by other group members abroad
- Provisions for informing data subjects about the BCRs and the transfers
- Training policies for employees handling personal data
- Duties of the persons or teams responsible for handling requests and monitoring compliance
- Audit mechanisms
- Reporting obligations for updates to the BCRs and notification to the Board
- Obligations to cooperate with the Authority
- A declaration that no conflicting national laws exist in the recipient country and that the Board will be notified of any legislative changes that may undermine the safeguards
- A commitment to provide continuous data protection training to employees with regular access to personal data

3) Standard Contract

Data exporters and foreign data importers can rely on a Standard Contract published by the Board.

- The contract must be signed without any amendments to its content.
- Although the Board publishes an English translation for reference, only the Turkish text is legally binding.

The signed contract must be submitted to the Board within five business days by one of the following methods:

- Physical submission
- Registered electronic mail (KEP)

- The Standard Contract Notification Module at <https://standartsozlesme.kvkk.gov.tr>

The parties must identify who is responsible for notifying the Board. If not stated, the responsibility lies with the data exporter.

Any changes to the parties, the details of the data transfer, or termination of the contract must also be reported to the Board.

4) Undertaking (Commitment Letter)

Data exporters and data importers may also provide safeguards by signing a written undertaking (*taahhütname*), subject to the Board's approval.

- If submitted in a foreign language, the Board will base its decision on the Turkish version.

The undertaking must include at least the following:

- The purpose, scope, nature, and legal basis of the data transfer
- Definitions of key terms
- A commitment to the core principles of the KVKK
- Provisions to inform data subjects about the transfer and the undertaking
- A commitment to uphold data subject rights
- A commitment to implement technical and administrative security measures
- Restrictions on onward transfers
- Legal remedies available to the data subject in the event of a breach
- A commitment to comply with the Board's decisions and opinions

- A declaration that no conflicting national legislation exists, and an obligation to notify the exporter of any changes granting the right to suspend or terminate the transfer
- A commitment by the importer to return or permanently delete all transferred personal data and backups upon termination or expiry of the undertaking
- A clause confirming that the undertaking is governed by Turkish law, that Turkish courts have jurisdiction, and that the data importer accepts this jurisdiction

Exceptional Transfers of Personal Data Abroad

Personal data may be transferred abroad without an adequacy decision or appropriate safeguards, provided that the transfer is occasional and one of the following exceptional conditions applies.

Conditions for a Transfer to Be Considered Occasional

The transfer must:

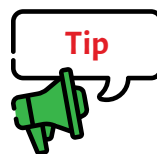
- Not be regular
- Occur once or only a few times
- Not be continuous
- Not take place in the ordinary course of business

Exceptional Transfer Grounds:

An occasional transfer of personal data abroad may be permitted under the following circumstances:

- The explicit consent of the data subject has been obtained, and the individual has been informed of the potential risks
- The transfer is necessary for the performance of a contract between the data subject and the data controller, or for taking pre-contractual steps at the request of the data subject

- The transfer is necessary for the conclusion or performance of a contract entered into in the data subject's interest, between the data controller and another natural or legal person
- The transfer is necessary for reasons of overriding public interest
- The transfer is necessary for the establishment, exercise, or defence of a legal claim
- The transfer is necessary to protect the life or physical integrity of the data subject or another person where the data subject is physically or legally incapable of giving consent
- The data is transferred from a public register that is open to the public or accessible to persons with a legitimate interest, in accordance with applicable law



→ To meet the obligation of informing the data subject of potential risks, they must be made explicitly aware that their personal data is being transferred to a country without an adequate level of protection, and that data security safeguards in that country may be insufficient.

Rights of Data Subjects and Legal Remedies



Rights of Data Subjects and Legal Remedies

Rights of Data Subjects

Under the KVKK, data subjects are entitled to the following rights:

- To learn whether their personal data is being processed
- If it is being processed, to request information about such processing
- To learn the purpose of processing and whether their data is being used in line with that purpose
- To know the third parties to whom their data has been transferred, either domestically or abroad
- To request the correction of incomplete or inaccurate personal data
- To request the erasure or destruction of personal data
- To request that third parties to whom the data has been transferred are informed of any corrections, erasures, or destruction
- To object to outcomes arising to their detriment from automated processing carried out exclusively through automated systems
- To claim compensation for damages resulting from the unlawful processing of personal data

Application to the Data Controller

Data subjects may exercise their rights by submitting a request directly to the data controller. In accordance with the *Communiqué on the Principles and Procedures for Application to the Data Controller*, the application must:

- Be in Turkish
- Include the data subject's name and surname, signature (if submitted in writing), Turkish ID number (or passport number for foreign nationals), address or electronic notification address, telephone/fax number, and a clear statement of the request
- Optionally include relevant supporting documents and information

Requests may be submitted through:

- Written application
- Registered electronic mail (KEP)
- Secure electronic signature
- Mobile signature
- An email address previously provided to the data controller by the data subject
- A software or application developed for handling such requests

The data controller must respond within 30 days, either accepting the request or rejecting it with justification.

Complaint to the Board (KVKK Authority)

A data subject may not file a complaint directly with the Board without first applying to the data controller. If the data controller:

- Rejects the request
- Provides an inadequate response
- Fails to respond within 30 days

...the data subject may then lodge a complaint with the Board.

Complaints must be submitted:

- Within 30 days of receiving the controller's response, and,
- In any event, no later than 60 days from the original application date.

Board Investigations

The Board may initiate an investigation:

- Upon receiving a complaint, or,
- Ex officio upon learning of a potential personal data breach.

The data controller must:

- Provide all requested documentation
- Allow on-site inspections, if deemed necessary

The Board must issue a decision within 60 days. If no response is provided within that period, the request is deemed rejected. In either case (explicit rejection or no response), the data subject may file an annulment action before the administrative courts.

If a violation is found, the data controller must remedy the breach within 30 days. Sanctions may include:

- Administrative fines
- Suspension of processing
- Deletion or anonymisation of the personal data

The controller may appeal the Board's decision before the administrative courts in Ankara, within 60 days, in accordance with the Administrative Procedure Law.

Right to Compensation

According to Article 14(3) of the KVKK:

“Data subjects whose personal rights have been violated retain the right to compensation under general legal provisions.”

The KVKK Guide on Legal Remedies clarifies that a data subject may also file a direct lawsuit in court without first applying to the data controller or the Board.

While applying to the controller is a prerequisite for submitting a complaint to the Board, it is not required to pursue a civil claim through the courts.

Key Court Decisions

Turkish Court of Cassation – 4th Civil Chamber

Decision dated 08/05/2019, File No. 2019/979, Decision No. 2019/2679:

*In a case where a mobile line was unlawfully registered in the plaintiff's name, leading to a debt collection process, the court held both the telecom company and its dealer jointly liable. The unauthorised processing of identity data was ruled a violation of personality rights, and the court awarded both **material and moral damages**.*

Court of Justice of the European Union – Case C-687/21:

The CJEU ruled that even the fear or concern that one's personal data may be misused by third parties is sufficient to justify a claim for non-material (moral) damages. This reinforces the principle that personal data protection covers not only actual harm but also intangible effects such as emotional distress or reputational anxiety.

Relevant Legislation

The Personal Data Protection Law

By-Law on Erasure, Destruction or Anonymization of Personal Data

By-Law on the Procedures and Principles for the Transfer of Personal Data Abroad

By-Law on Data Controllers Registry

Communique on Principles and Procedures to Be Followed in Fulfilment of the Obligation To Inform

Communiqué on the Principles and Procedures for the Request to Data Controller

Contacts



Deniz Eray Harvey

deniz@harveyarasan.com

[linkedin.com/in/denizerayharvey/](https://www.linkedin.com/in/denizerayharvey/)



Eren Arasan

eren@harveyarasan.com

[linkedin.com/in/eren-arasan/](https://www.linkedin.com/in/eren-arasan/)

Harvey Arasan

İstanbul: Şakayık Sok. No.32 D.10 K.7 Teşvikiye, Şişli, 34365

Paris: 11 Boulevard de Sébastopol 75001 Paris

Tel: +90 212 931 77 48

www.harveyarasan.com

info@harveyarasan.com

www.linkedin.com/company/harveyarasan/

HARVEY ARASAN

This Guide has been prepared solely for informational purposes and in accordance with the Attorneys' Act No. 1136 and the Professional Rules of the Union of Turkish Bar Associations, including the regulations prohibiting attorney advertising.

The information, commentary, and evaluations contained herein do not constitute legal advice or a legal opinion specific to any case or client. No attorney-client relationship is formed through the use of this Guide. Harvey Arasan and its affiliated attorneys disclaim any liability for actions taken or not taken based on the contents of this publication without obtaining appropriate legal counsel. This document is intended to promote general awareness on legal matters and is not a substitute for tailored legal services.

All text, graphics, tables, and other content contained in this Guide — including the Harvey Arasan logo — are the intellectual property of Harvey Arasan. These materials may not be modified or used for commercial purposes without prior written permission. However, the Guide — in whole or in part — may be shared or reproduced for personal, institutional, or educational purposes, provided that proper attribution is given.

For further information or to share your feedback regarding this Guide, please contact us at info@harveyarasan.com