YAZICIOGLU LEGAL

A New Year's Gift from the Turkish Data Protection Authority: The Guideline on Transferring Personal Data Abroad Has Been Published!

January 7, 2025

On the second day of the new year, the Turkish Data Protection Authority (**Authority**) published the long-awaited Guideline on Transferring Personal Data Abroad (**Guideline**), eagerly anticipated by practitioners and stakeholders in this field.

As you may know, significant amendments were made to the Turkish Data Protection Law (**DP Law**) in 2024 as part of efforts to align the legislation with the European Union General Data Protection Regulation (**GDPR**). These changes substantially reformed the regime for transferring personal data abroad. Subsequently, the Authority issued the Regulation on Procedures and Principles Regarding the Transfer of Personal Data Abroad (**Regulation**), alongside draft templates for standard contractual clauses (**SCCs**) and binding corporate rules (**BCRs**), detailing the new regime.

(You can access our previously prepared infographic note on the amendments introduced by the DP Law and the Regulation here.)

Following these developments, many data controllers and data processors, obligated to comply with the new regime by September 1, 2024, accelerated their efforts, particularly concerning SCCs and BCRs. However, varying interpretations of the new provisions in the DP Law and Regulation among practitioners led to numerous uncertainties in practice.

Many were aware that the Authority was preparing a guideline to address these uncertainties and ensure uniformity in practice, particularly regarding the drafting of SCCs under the new regime. As a result of these efforts, the Guideline was shared with the public last Thursday, January 2.

Below, we have summarized the key highlights of the Guideline that caught our attention.

A. Scope of the DP Law

- **The DP Law's "Broad" Territorial Scope:** For some time, it has been thought that the Authority has applied the principles of territorial applicability found in the Misdemeanors Law and the Turkish Penal Code to determine the scope of the DP Law. This approach was supported by some unpublished Authority decisions. For the first time, the Guideline publicly confirmed the Authority's stance on this matter.

  Accordingly, if the relevant act is committed partially or entirely in Turkiyeor if the result occurs in Turkiye, the offense/misdemeanor is considered to have been committed in Turkiye (the principle of territoriality). The guide emphasizes that for this principle to apply, it is not necessary for the act and the result to occur in the same country; the place where the act is performed and the place where the result occurs may differ. From this perspective, it may be concluded that the processing of data of individuals located in Turkiye by foreign data controllers is subject to the DP Law.

The Authority, while emphasizing that the principle of territoriality should be interpreted broadly, referred to the Authority Decision on Procedures and Principles Regarding Data Breach Notifications, stating:

"In cases where a data breach occurs under a data controller established abroad, and the consequences of this breach affect data subjects residing in Turkiye who benefit from products and services offered in Turkiye, it has been decided that such data controllers must notify the Authority *within the same framework of rules."*

Based on this statement, the Authority highlighted that the territorial scope of the DP Law is interpreted not through "the principle of territoriality", but rather through the "principle of effect".

Our Comment: In our opinion, there is a contradiction between these two statements. The phrase *"consequences of this breach affect data subjects residing in Turkiye"* could already be interpreted as *"the consequence occurring in Turkiye"* within the framework of the broadly interpreted principle of territoriality. However, the Authority may have intended to state that even when the consequence does not occur in Turkiye, the DP Law would still apply based on the principle of effect.

Nonetheless, the introduction of the new concept of the "principle of effect" raises uncertainties about its conditions of application and when the effect would be considered to have occurred, which has the potential to spark various debates. In our view, considering only the *"broadly interpreted principle of territoriality"* would be more accurate from a legal interpretation perspective.

Additionally, we believe that the Authority's reference to *"the principle of effect"* rather than *"the principle of targeting"* is a deliberate choice, signaling its intent not to fully align with the GDPR in this respect.

In any case, it is evident that the Authority aims to interpret the DP Law in a manner that allows for the broadest possible geographical scope of application.

- **"Broadly" Interpreted Concept of Transfer:** The act of transferring or making personal data accessible by the data exporter has been illustrated with various examples. Activities such as creating an account, granting access rights to an existing account, approving or accepting an effective request for remote access, placing a hard drive, or sending a password for a file have been provided as examples of personal data transfers. Notably, it is stated that in cases of data viewing conducted from abroad during support services provided for troubleshooting or management purposes, personal data will be considered transferred abroad if other criteria are met.

B. Direct Collection Does Not Constitute a Transfer Abroad

The Authority has explicitly stated that activities involving the direct transmission of personal data by the data subject to an entity located abroad, where no intermediary data exporter exists between the data subject and the entity collecting the data, cannot be considered as a transfer of personal data abroad.

This assessment by the Authority is essentially aligned with the definition of *"transfer of personal data abroad"* provided in the Regulation. The Regulation's definition emphasizes the necessity of a relationship between a data exporter and a data importer for an activity to be regarded as a transfer of personal data abroad.

The examples provided by the Authority highlight that while direct collection activities do not constitute a transfer abroad, onward transfers of the collected data must be separately evaluated. In this context, it is clearly stated that if the directly collected personal data is transferred to a data importer (data controller/processor/sub-processor) located in a country other than Turkiye, the provisions of the DP Law regarding the transfer of personal data abroad will apply.

- **Collection and Transfers by a Data Controller Subject to the DP Law in a Third Country:** While the Guideline reiterates that the direct collection of personal data is not considered a data transfer abroad under the DP Law, it also clarifies that a data controller subject to the DP Law will still be bound by the provisions governing transfers abroad. This explanation resolves the uncertainties raised by its decision on WhatsApp, where the Authority referred to direct collection as a data transfer abroad.

  The Guideline explicitly states that when a data controller in a third country subject to the DP Law transfers personal data to another country outside Turkiye, the provisions of the DP Law on transfers abroad must apply. For example, the Guideline presents a scenario where a person residing in Turkiye enters their name, surname, and email address into a form while purchasing a bag online. If the website is operated by a third-country company not established in Turkiye but targeting the Turkish market, and the company also processes the orders, this would be considered direct collection of personal data. However, if the collected data is subsequently transferred to a data processor outside Turkiye, this would qualify as a data transfer. In such cases, the provisions of the DP Law on transfers abroad will apply. Importantly, the Guideline emphasizes that in this example, the data processor being located in the same country as the data controller does not make a difference; the fact that the data is processed outside Turkiye is sufficient to classify the situation as a transfer abroad (the Guideline, Section 4(A), Example-2).

- **Transfers Within Group Companies:** One of the highly anticipated issues in practice was how data sharing between a subsidiary and its parent company, particularly within group companies, would be evaluated.

  In the Guideline, the Authority clarified that if a subsidiary transfers employee data to a parent company located in a third country for storage in a centralized human resources database, the subsidiary processes this data as an employer and consequently a data controller. In this scenario, the parent company is considered a data processor (the Guideline, Section 4(A), Example-7).

Our comment: Although the example does not provide the level of clarity we had hoped for, we believe it may serve as a basis for structuring cases where a parent company signs a contract with service providers to obtain services and makes these services available for use by its subsidiaries or sub-group companies:

- The sub-group company could be positioned as the data controller,
- The parent company as the data processor, and
- The service provider companies as the sub-processors.

C. Initial Assessment: Provisions on Cross-Border Data Transfers in International Treaties and Laws

The Guideline states that if there is a provision in international treaties or other laws concerning cross-border data transfers, personal data may be transferred in accordance with these provisions.

In this context, it is emphasized that, as the first step in cross-border data transfers, it should be assessed whether there is a relevant provision in international treaties or other laws before considering adequacy decisions, appropriate safeguards, or occasional transfer conditions.

In fact, this point was previously highlighted in the Authority's Good Practice Guideline for the Banking Sector on the Protection of Personal Data. It was noted that the "*specific provisions on cross-border personal data transfers*" in the Banking Law would take precedence over the general provisions of the DP Law.

Our Comment: This approach, as emphasized in the Guideline, is seen as a facilitating factor for regulated sectors governed by special laws that involve cross-border personal data transfers. For instance, the example provided in the Guideline refers to certain articles of the Law on the Prevention of Laundering of Criminal Proceeds -although these articles are no longer in force-. Therefore, even if there is no special law regulating a particular sector, any provision in any law concerning cross-border personal data transfers will take precedence, and the general cross-border transfer rules of the DP Law will not apply. This means that it will not be necessary to provide safeguards such as standard contracts, for certain transfers regulated by other laws.

D. Occasional Transfers

One of the most significant changes introduced by the new transfer regime is the possibility of cross-border data transfers without requiring prior authorization from the Authority, provided that the transfer is occasional -meaning it occurs on a one-time or occasional basis, is not continuous, and does not take place as part of ordinary business operations- in cases where neither an adequacy decision nor one of the appropriate safeguards is available.

However, there have been differences of opinion in practice regarding what types of transfers can be considered occasional transfers. Here are the key points highlighted in the Guideline to resolve such differences of opinion:

- **Occasional Cases:** Data transfers conducted in occasional cases should be regarded as exceptional and interpreted very narrowly.

According to the Guideline, transfers that occur regularly as a result of an ongoing relationship between the data exporter and the data importer are considered systematic and repetitive transfers and, therefore, do not fall within the scope of occasional transfers.

Example:

Granting direct access to a database to a data importer is considered a regular and continuous transfer and cannot be deemed an occasional transfer.

The Guideline also emphasizes that occasional transfers may occur more than once. However, for such transfers to be classified as occasional, they must not be regular, must not exhibit continuity, must occur under unforeseen circumstances, and must take place at irregular intervals outside the ordinary course of business operations.

Example:

If a tourism company shares its customers' reservation information, such sharing would not qualify as an occasional transfer, as it is part of the company's routine business processes and is performed regularly by the nature of its operations.

- **Relying on Explicit Consent for Occasional Transfers:** Explicit consent must be obtained before the cross-border transfer takes place. However, in cases where the transfer is not foreseeable, consent should not be preemptively obtained with a "just in case" approach. Consent must be provided at the moment the transfer is anticipated and specifically for that transfer.

  Explicit consent for occasional transfers must include the following elements:

  - ✓ The identity of the data exporter,
  - ✓ The purpose of the transfer,
  - ✓ The specific type of personal data being transferred (not just the category, the specific data),
  - ✓ That explicit consent can be withdrawn,
  - ✓ That explicit consent constitutes a legal basis for the transfer,
  - ✓ That no adequacy decision exists for the destination country,
  - ✓ The potential risks of the transfer.

  Additionally, data subjects must be informed that their personal data will be transferred to a country that does not provide adequate protection. They must be explicitly informed about the lack of sufficient safeguards for data protection in that country and the specific risks arising from this situation.

E. Drafting Standard Contractual Clauses

Although the Authority has published SCCs to be used in cross-border data transfers, some uncertainties arose in practice in terms of the preparation of these contracts. With the published Guideline, some of these uncertainties have been clarified.

In this context:

- It is stated that the contracts can be drafted in a dual-column, bilingual format, but in any case, the Turkish text will be taken as basis.
- Although the relevant heading in SCCs includes the phrase “Personal Data Categories”, it is seen that the explanation given by the Authority in the relevant section includes personal data types in addition to the data categories. Therefore, it can be said that the Authority will not consider it sufficient to include only personal data categories and personal data types must also be included.
- It has been stated that the types of personal data transferred must be matched to indicate which group(s) of data subject(s) they relate to.
- In addition to the purposes for the cross-border data transfer by the data exporter, the processing purposes of the data importer should also be included.
- Contracts must be concluded between the parties to the transfer.
- It is stated that if official documents obtained from a foreign country are used in contract notifications (if obtained from a country that is a party to the Convention on the Abolition of the Obligation to Certify Foreign Official Documents), an apostille stamp must be obtained, otherwise, it will be expected to obtain certification from the consulate or diplomatic officers in the relevant country for the relevant documents.
- It is stated that it is necessary to specify which legal basis under the Law is relied upon the for the transfer.

  Our comment: There has been an ongoing debate since amendment to the DP Law: *“Should we determine a separate legal basis for the cross-border transfer, or does the legal basis for the main processing activity also apply to the transfer?”* Unfortunately, the Guideline do not seem to provide a clear answer. However, we are of the opinion that at least in the “Legal basis for the transfer” section of the SCCs, it can be interpreted that a legal basis for the transfer must be written, and that the legal basis for the main processing activity is not expected to be written in that section. However, it would be very useful for the practitioners to clarify this issue in the updates of the Guideline.

F. Binding Corporate Rules

The Guideline states that personal data may be transferred abroad only if the BCRs application to the Authority is approved by the Authority. Therefore, as in the case of applications for approval of written undertakings in the old transfer system, there may be a risk of sanctions if the transfer activities are initiated before the approval of the Authority.

However, the Guideline also emphasizes that the approval granted by the Authority does not mean that the Authority has assessed whether each data processing activity complies with all the requirements of the DP Law and that the data exporter must make sure that the requirements of the DP Law are met for each transfer activity.

In addition, the Guideline states that if the headquarters of the group of companies is located in Turkiye, the application must be made by this headquarters or by another organization located in Turkiye to which the responsibilities regarding the protection of personal data are

transferred under certain conditions, together with additional grounds as to why this organization is designated as the applicant.

If the headquarters of the group is located outside of Turkiye, the group must appoint a group entity located in Turkiye as the authorized group member to whom the responsibilities regarding the protection of personal data are delegated, and this authorized entity must then submit the application to the Authority on behalf of the group.

You can reach the Turkish version of the Guideline from here.

Please do not hesitate to contact us if you have any questions.

Kind regards,

Bora Yazıcıoğlu

bora@yazicioglulegal.com

Nafiye Yücedağ

nafiye@yazicioglulegal.com

Emre Öntekin

emre@yazicioglulegal.com

Barış Aslan

baris@yazicioglulegal.com

This information note does not constitute legal advice. It has been prepared and shared solely for informational purposes. If you wish to obtain legal advice on this matter, please do not hesitate to contact us.