Türkiye Introduces New Rules

for Cross-Border Transfers of Personal Data – Key Takeaways

**Introduction**

The Turkish Parliament has passed the law amending the Law on the Personal Data Protection numbered 6698 (“**PDPL**”) with the aim to align the relevant cross-border rules with those of the European Union General Data Protection Regulation (“**GDPR**”). The changes were adopted on 12 March 2024, with effect from 1 June 2024.

As part of the amendments, the Turkish Data Protection Authority (“**Authority**”) published the Regulation on Cross-Border Transfers of Personal Data (“**Regulation**”) in the Official Gazette on 10 July 2024 with immediate effect1. This piece of legislation provides a structured framework for managing international data transfers. So, companies transferring customer data overseas now need to adhere to the new procedures to ensure compliance.

Below we list key takeaways from the changes to the Turkish data protection regime.

**Key Provisions of the Regulation**

**Introduction of New Definitions**

The Regulation introduces new definitions for terms including “Cross-Border Transfer of Personal Data,” “Data Exporter,” and “Data Importer”, which were previously not defined in the legislation, providing much-needed clarity and a structured framework for managing cross-border data transfers.

**Adequacy Decisions**

The Regulation details the criteria for the Authority to issue adequacy decisions, recognizing that certain countries, sectors, or international organizations provide a level of data protection comparable to that of Türkiye. These decisions are to be re-evaluated every four years, ensuring ongoing compliance with evolving data protection standards. The criteria include the existence of independent and effective data protection authorities, the legal framework and its application in the recipient country, the availability of administrative and judicial redress, the country or organization’s adherence to international data protection agreements, the reciprocity status between Türkiye and the recipient, and the membership or adherence to international agreements related to data protection.

**Safeguards for Transfers Based on Appropriate Measures**

In the absence of an adequacy decision, the Regulation outlines the appropriate safeguards that can be used for data transfers, including Standard Contractual Clauses (“**SCC**”), Binding Corporate Rules (“**BCR**”), approved undertakings, and specific international agreements that are not considered treaties but involve cooperation between public institutions or professional organizations. These measures are expected to provide enforceable data subject rights and effective legal remedies. The Regulation ensures that data subjects have the same level of protection and rights, regardless of where their data is transferred.

* **Rules on Standard Contractual Clauses (SCCs)**

The Regulation provides comprehensive guidelines on the execution and notification of SCCs. Within 5 days of signing, SCCs are required to be reported to the Authority either by hand, through registered e-mail (*Kayıtlı Elektronik Posta* - KEP), or via other methods specified by the Authority. The Regulation requires that any changes to the SCCs, such as modifications, changes in the parties involved, or termination, must be reported to the Authority. It is important to note that the SCCs cannot be altered, and any attempts to do so or the absence of valid signatures will trigger an official examination by the Authority. This strict adherence ensures the integrity and enforceability of SCCs in maintaining data protection standards. The SCCs include provisions on the categories of data, the purposes of the transfer, the recipients and recipient groups, the technical and organizational measures taken by the data importer, and additional safeguards for special categories of personal data. With the Authority's release of the final versions of the SCCs on July 10, 2024, companies now have a robust framework to ensure compliant cross-border data transfers. This seamless framework allows organizations to navigate the complexities of data transfer regulations effectively. Transitioning to another critical aspect, multinational companies often need more tailored solutions, leading us to the importance of BCRs.

* **Binding Corporate Rules (BCRs)**

For multinational companies, the Regulation specifies the process for obtaining Authority approval for BCRs, which offer a more flexible and comprehensive solution for global data transfers. These rules must include provisions that ensure adequate protection for data transferred within a corporate group. BCRs must be legally binding and enforceable across all relevant entities, ensuring a consistent level of data protection. The Regulation outlines the minimum content requirements for BCRs, ensuring they provide adequate safeguards for international data transfers within corporate groups. Applications for BCR approval must include the BCR document and any other necessary information and documents, including notarized translations if the documents are in a foreign language. The Authority will review the BCRs based on criteria such as legal bindingness, enforceability across the corporate group, and compliance with the specified content requirements. Furthermore, on July 10, 2024, the Authority issued draft templates and guidelines for BCR applications, further supporting companies in achieving compliance with cross-border data transfer requirements.

* **Undertaking Applications**

The Regulation specifies the minimum required content for undertakings that data controllers and processors must submit to the Authority for approval. These undertakings must include comprehensive details to ensure adherence to stringent data protection standards. The provisions must cover the purpose, scope, nature, and legal basis of the data transfer, definitions in line with relevant laws, compliance with general principles of data processing, procedures for informing data subjects, and measures for allowing the exercise of their rights. Additionally, the undertakings must outline the technical and administrative safeguards, additional measures for special categories of data, restrictions on further transfers, remedies for data subjects in case of breach, and compliance with Authority's decisions. The data recipient must also commit to informing the data exporter about any conflicting national regulations, allowing the suspension of the transfer and termination of the undertaking if necessary.

**Conditions for Non-Repetitive Transfers**

In situations where there is no adequacy decision or alternative safeguards, the Regulation permits the transfer of personal data abroad under specific non-repetitive circumstances. Such transfers must not be part of regular business operations, should occur only occasionally, and must not represent ongoing activities. This provision ensures that exceptional transfers remain controlled and do not become a regular practice.

**Responsibilities of Data Processors**

The Regulation underscores the obligation of data controllers to verify that data processors adopt adequate security measures. Additionally, it requires data processors to inform the Authority about the implementation of an SCC, regardless of direct instructions from the data controller, enhancing accountability. This provision ensures that data processors uphold the same level of data protection as data controllers.

**Enforcement and Compliance**

The Authority has the power to conduct inspections to ensure compliance with the Regulation. Failure to comply can lead to substantial penalties, emphasizing the importance of adhering to the new rules. According to the amended PDPL, failure to fulfill the notification obligation to the Authority regarding the execution of SCCs within five business days can result in significant administrative fines. Companies must ensure they have robust data protection measures in place to avoid these penalties. The Authority’s enforcement powers include the ability to suspend data transfers, impose fines, and require corrective actions.

**Conclusions**

The new Regulation marks a significant step towards aligning Turkish data protection laws with international standards. Companies engaging in cross-border data transfers must carefully review and comply with the provisions of the Regulation to ensure smooth and lawful data operations. Staying up-to-date with the latest developments and maintaining stringent data protection practices are crucial for managing cross-border data transfers in this complex regulatory environment. A proactive approach will help companies build trust with their customers and ensure compliance with both Turkish and international data protection standards.

**Footnotes**

1 <https://www.resmigazete.gov.tr/eskiler/2024/07/20240710-2.htm>