TURKEY'S DATA PRIVACY LEGISLATION AND ITS COMPLIANCE WITH GLOBAL REGULATIONS

Turkey's legislative journey regarding personal data protection was initiated in 1981, when it signed the Council of Europe's Convention No. 108. Since then, the world economy has transformed into a data-driven economy, in which the free flow of data is crucial in maintaining economic relations. As a result, trade sectors have been increasingly relying on cross-border data transfers, and therefore need a less restrictive and functioning cross-border transfer mechanism without compromising on data protection and privacy. This article assesses Turkey's data privacy legislation within the context of international regulations, and explains what it needs to do to meet global standards.

Yasin Beceni*

TPQ
Fall 2020

* Yasin Beceni is Managing Partner at BTS & Partners.

Turkey's journey regarding the legislative actions on personal data protection has commenced with the Council of Europe's (CoE) Convention No. 108 of 1981 on the Protection of Individuals with regard to Automatic Processing of Personal Data. Although Turkey was one of the founding signatories of the Convention 108 as of 28 January 1981, its ratification and the enactment of a domestic personal data protection law were initiated with the EU accession talks. During the accession talks, four chapters, especially Chapter 23: Judiciary and Fundamental Rights and Chapter 24: Justice, Freedom and Security, required enactment of a law. In addition to requiring a law and establishing an independent data protection supervisory authority, the EU has also invited Turkey to initiate the ratification process of the Convention 108. As a response to these calls, Turkey has promised to enact a data protection law and ratify the Convention 108 in the first half of 2016, and ratify the Additional Protocol to Convention 108 regarding supervisory authorities and transborder data flows ("Additional Protocol 181") afterwards, in its National Action Plans for EU accession.

In this regard, there have been certain regulations, before the enactment of the Personal Data Protection Law (DPL), which aim to secure the privacy of data subjects in Turkey. One of these is Article 20 of the Turkish Constitution, which was introduced in 2010 and set the framework of the right to privacy; the other is provisions included in the Turkish Criminal Code, which envisage sanctions regarding unlawful recording and obtaining of personal data. Thus, before the introduction of the DPL to the Turkish legislation, the data protection in Turkey was based on the several articles of the Constitution and the Turkish Criminal Code. As a result of the promises given, Turkey ratified the Convention 108 in May 2016. The Law on the Ratification of the Convention 108 entered into force on September 2016, while the Additional Protocol 181 entered into force in November 2016, 35 years after signing the Convention 108.

After being prepared in line with the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Directive"), the DPL entered into force on 7 April 2016. A two-year period was granted to comply personal data processing activities that had been conducted before this date with the DPL.

Need for Improvement

While Turkey has adopted the DPL in accordance with the principles set in the Convention 108 and the Directive, the EU and CoE's data protection principles have been improved with the introduction of the Regulation (EU) 2016/679 of

the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation-GDPR) and the modernized Convention 108. This issue has been raised in European Commission's Turkey 2019 Report.[1] In the report, it is stated that the Personal Data Protection Authority ("Authority") has become operational and the Personal Data Protection Board ("Board") has been appointed, however, no legislative changes have taken place to ensure that the law is harmonized with the EU acquis, in particular with the GDPR and the Law Enforcement Directive 2016/680. The report has also particularly emphasized that Turkey has not signed or ratified the modernized Convention 108.

In this regard, both the 11th Development Plan and the Annual Program of the Presidency for the Year 2020 envisage that the legislation on protection of personal data will be updated in line with the innovations brought by technology and new approaches adopted on international platforms, and technological development in this field will be encouraged. More specifically, both strategic documents state that the DPL will be updated in accordance with the GDPR.

Turkey's Compliance with Global Data Privacy Regulations: General Terms

Turkey's introduction and implementation of the DPL has been quite harmonized with the Convention 108's requirements, except for the data transfer regime envisaged under DPL. Accordingly, some of the main principles that were adopted from the Convention 108 by the DPL are examined below.

General Principles

Requirements envisaged in the Article 5 of the Convention 108 are almost exactly reflected in the DPL under "General Principles", which explicitly regulate that the following principles shall be complied within the processing of personal data:

- Lawfulness and fairness
- Being accurate and kept up to date where necessary
- Being processed for specified, explicit, and legitimate purposes
- Being relevant, limited, and proportionate to the purposes for which they are processed
- Being stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data are processed

[1] European Commission, "Turkey 2019 Report," 29 May 2019, https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-turkey-report.pdf

Special Categories of Data

In addition to those already regulated under Article 6 of the Convention 108, the DPL also regulates appearance, membership to associations, foundations or trade-unions, security measures, and biometric and genetic data as special categories of personal data.

In principle, the DPL regulates that explicit consent of the data subjects are required for the processing of special categories of data. DPL then makes a distinction between data concerning health and sexual life, and other special categories of data in terms of conditions for processing. Accordingly, while the personal data concerning health and sexual life may only be processed by those having secrecy obligation or competent public institutions and organizations, other types of sensitive data can be processed in the cases provided for by other laws. Moreover, to determine the appropriate safeguards, the Board has also rendered a decision, which explains the necessary technical and organizational measures to be taken while processing special categories of data.[2]

Data Security

As required by the Convention 108, the DPL also sets forth that the data controller is obliged to take all necessary technical and organizational measures to provide an appropriate level of security for purposes of preventing unlawful processing of personal data, unlawful access to personal data, and ensuring protection of personal data. The Authority has also published the Data Security Guide[3] in order to further detail the said measures. While the DPL requires data controllers to take such measures, it also determines that the necessary audits shall be carried out for the implementation of this requirement.

Additional Safeguards for the Data Subject

To enable data subjects to have control over their data, the DPL grants certain rights, which are in line with Article 8 of the Convention 108. Accordingly, the data subjects have the right to:

[2] Personal Data Protection Authority, "'Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler' ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı [The Decision of the Personal Data Protection Board dated 31/01/2018 and numbered 2018/10 regarding 'Adequate Measures to be Taken by Data Controllers in the Processing of Special Quality Personal Data']," https://kvkk.gov.tr/Icerik/4110/2018-10

[3] Personal Data Protection Authority, "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) [Personal Data Security Guidelines (Technical and Administrative Measures)]," January 2018, https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf

- Request to learn whether his/her personal data are processed or not, the purpose of the processing of his/her personal data and whether these personal data are used in compliance with the purpose
- Demand information as to whether his/her personal data have been processed
- Know the third parties to whom his personal data are transferred within the country or abroad
- Request the rectification of incomplete or inaccurate data, if any
- Request the erasure or destruction of data in the event that the data is no longer necessary in relation to the purpose for which the personal data was collected, and request such processes to be notified to third persons to whom personal data is transferred
- Object to the occurrence of a result against the person himself/herself by analyzing the data processed solely through automated means
- Claim compensation for the damage arising from the unlawful processing of data

Co-operation between States and Supervisory Authorities

In order to enable mutual assistance and cooperation between states and to fulfill the obligation of appointing an independent authority responsible for ensuring compliance as envisaged under the Convention 108 and Additional Protocol 181, the DPL has established the Authority, which is a public legal entity and has administrative and financial autonomy, responsible for both the implementation of the DPL and cooperation at the national and international level. In this regard, the Board, which is the decision-making body of the Authority, is designated as the supervisory authority with respect to Convention 108.

Comparison of GDPR and the DPL

While the Convention 108 is the most widely adopted and binding regulation in the global arena, recently the GDPR has become the most distinctive and leading international instrument related to personal data protection and privacy. The GDPR encourages the adoption of several data protection regulations around the world through introducing the highest standards with its extraterritorial scope.

As the DPL was prepared based on the Directive repealed by the GDPR, there are many overlaps between the GDPR and the DPL in terms of general principles of processing, definitions, as well as certain conditions of processing.

On the other hand, although there are certain overlaps, the obligations attributed to

data controllers and data processors under GDPR and DPL differ significantly. While most of the statutory requirements attributed to data processors and controllers are not present under the DPL, the most important implication of DPL concerning legal responsibilities of data processors and controllers is under the scope of data security provisions. Some of the distinctions are listed below:

- GDPR foresees a detailed procedure and mandatory contractual provisions to be complied when a controller appoints a data processor. Whereas the DPL lacks such clear requirements. In any case, getting into a detailed data processing agreement with the processors may be deemed as a step taken in order to comply with the obligation of data controllers in taking all necessary organizational and technical measures in ensuring adequate security for personal data processed.
- Unlike under GDPR, data processors are not legally under the obligation to cooperate with the Authority (e.g., provide information or documents; allow for on-site auditing) while data controllers are.
- The obligation to appoint a DPO is not present for both controllers and processors under the DPL.
- The scope legal liability of processors against data subjects is much limited under DPL, when compared to GDPR. For examples, data processors are not responsible in terms of cross-border data transfer procedures under DPL. Data controllers are the sole responsible.

Turkey's Compliance with Global Data Privacy Regulations: Cross-Border Data Transfer

In Turkish legislation, although cross-border transfer of personal data is not explicitly prohibited, due to the strict and impractical pre-conditions anticipated for such transfers, in practice, the private entities have only a limited space to realize cross-border transfers of personal data while carrying out their business operations. In this regard, the cross-border transfer of personal data is mainly regulated under the DPL. The DPL has set the framework of the rules to be followed when transferring personal data from Turkey to abroad through three mechanisms. Thus, the Article 9 of the DPL requires compliance to the either one of the options:

- **Obtaining explicit consent from the related data subjects**: The first option for the cross-border transfer of personal data is obtaining the explicit consent of the data subjects. In the event that the data subject gives his explicit consent, it will be possible for companies to transfer the personal data abroad without seeking any other conditions. However, in practice, this transfer mechanism is mostly suitable for companies dealing with relatively

small group of data subjects; otherwise, it is unfeasible for companies to operate on changing consent preferences, which have the potential to impose an overwhelming operational and financial burden to companies.

- **Transferring personal data to the countries determined by the Board as providing adequate level of data protection**: If the recipient country is indicated as a safe country under the list determined by the Board, the cross-border transfer to this country will be permitted, provided that a condition for the processing of personal data under DPL are fulfilled. In this case, the respective transfer operation is considered as having the same legal status with the transfer operation which is taking place within the borders of Turkey. However, although the DPL explicitly states that the list of countries providing an adequate level of personal data protection shall be declared by the Board, such list has not been published yet, which makes this transfer mechanism practically impossible for companies.

- **Receiving the Board's approval for the transfer made by the data controllers in Turkey to the data controller abroad**: In the event that a condition for the processing of personal data under DPL is fulfilled, a written undertaking agreement ensuring adequate protection between the data controllers in Turkey and abroad is concluded, and the Board's approval is received for the relevant cross-border data transfer. In this context, the Board has published the minimum contents required for these written undertakings to be concluded between transferring parties. However, in practice, while the engagements for obtaining the Board's approval for such transfers established by both local and foreign parties concluding the required undertaking, as confirmed by the Board, it has abstained from providing such approval so far, which eliminates the option to rely on this mechanism.

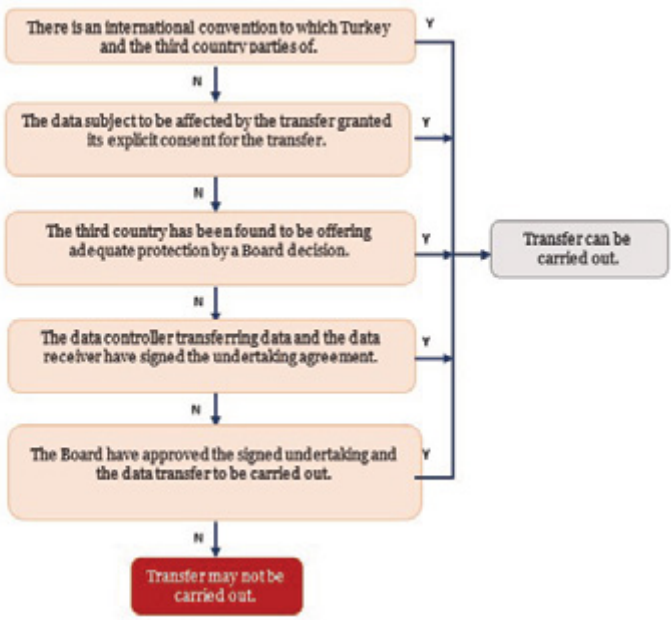
DPL also states that the provisions of other laws concerning the transfer of personal data abroad are reserved. Accordingly, in several regulations, certain institutions and organizations are authorized for realizing the cross-border transfer operations. The operations anticipated under these regulations are completely independent from the process stipulated in the DPL and, thus, the Board's permission is not required for said transactions.

In addition, the Article 90/5 of the Turkish Constitution envisages the prioritized applicability for international agreements that are duly put into effect and that concern fundamental rights and freedoms. Although there are many international agreements envisaging the transfer of personal data, the main international agreement regulating the cross-border transfer of personal data is the Convention 108. Since the Convention

108 and its Additional Protocol 181 have been duly signed by the Turkish government and are related to fundamental rights and freedoms, the provisions of this convention shall be applied in terms of cross-border data transfer operations with priority.

As an alternative method for the transfer of data between multinational group companies where there is no sufficient protection in the destination country, the Authority introduced the concept of Binding Corporate Rules (BCR). BCR may be submitted to the Board, and Board's approval must be obtained to transfer personal data legally, without the need to obtain explicit consent (in cases where processing of personal data may be made based on legal grounds other than explicit consent, e.g., execution of the agreement, exercise of legal rights, or fulfilling legal requirements).

Figure 1: Cross-Border Transfer of Personal Data between Turkey and a Third Country



Cross-Border Data Transfer Regime Under the Convention 108

Under the Convention 108, the parties are required to take the necessary steps in their domestic legislation to apply the principles the Convention foresees in order to ensure the fundamental human rights of all individuals with regard to processing of personal data.

Accordingly, the Article 12 of the Convention 108 determines the provisions, which shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed. Under these provisions, the Convention 108 explicitly states in the paragraph 2 of Article 12 that, in principle, a party to the Convention 108 shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another party. The Convention 108 also specifies the exceptions to the said rule in the following provisions:

"Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:

- insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;
- when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph."

Furthermore, Additional Protocol 181 foresees a new provision on cross-border data transfer operations by stating that each party of the Convention 108 may provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organization that is not a party to the Convention, provided that the State or organization ensures an adequate level of protection for the intended data transfer. Besides, the Additional Protocol No. 181 also envisages that by way of derogation in the aforementioned provision, each party may allow for the transfer of personal data if the domestic law (i) provides for it because of specific interests of the data subject or legitimate prevailing interests, or (ii) safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.

To conclude, in principle, the parties to the Convention 108 are permitted to transfer personal data among contracting states without the necessity for an approval from an authority or being bound by the list of countries with adequate protection.

Turkey's Stance Toward Convention 108 in Light of the Recent DPA Decision

As it can be seen from the above-specified concept of data transfer, the DPL does not

make a clear distinction between the countries that are parties to the Convention 108 and others; however, by prioritizing the implementation of international agreements regulating data transfers, the DPL grants opportunity to introduce a special regime for the parties to the Convention 108. In this regard, it has been argued that being announced as a safe country shall not be required for parties to the Convention 108, as international agreements on cross-border transfers are prioritized.

However, contrary to the main principle of Convention 108, which states that "the parties shall not prohibit or subject to special authorization transborder flows of personal data going to the territory of another party and that the parties may introduce additional safeguards in case the transfers are made to third countries," the Board's recent decision, dated 22 July 2020 and numbered 2020/559[4] ("Decision"), has disregarded the applicability of Convention 108 for data transfers from Turkey to Europe by arguing that the Convention 108 grants parties the right to restrict cross-border transfers in their domestic laws, which is implemented by Turkey in the DPL. Establishing that the Convention 108 cannot be a basis for transferring personal data abroad, the Board has also noted that being a party to the Convention 108 alone is not sufficient in determining the status of a safe country within the scope of DPL, but will constitute a positive element in the assessment to be made by the Board.

Rejecting the argument, which indicates that free flow of personal data among parties envisaged by the Convention 108 must prevail over the mechanism introduced by Article 9 of the DPL since the privacy and protection of private life is a fundamental right and Article 90/5 of the Turkish Constitution recognizes this prioritized applicability for international agreements that are duly put into effect and concerning fundamental rights and freedoms; the Board expressed its approach by stating that these agreements may only be directly implemented in case the related provisions are sufficiently clear, precise, unconditional, and do not require the states to take additional measures for its implementation; and as the Explanatory Report of the Convention 108 allows the states to introduce additional restrictions, the implementation of the Convention 108 cannot be considered within this scope.

As a result of the Decision, the practice of the DPL has been structured in a way that makes cross-border data transfer impossible, unless explicit consent is obtained from data subjects, or the Board's approval to the transfer—for which an undertaking is concluded between the data transferring parties—is received. This is contrary

[4] Personal Data Protection Authority, "'Kişisel verilerin 108 sayılı Sözleşme dayanak gösterilerek yurt dışına aktarılması hakkında' Kişisel Verileri Koruma Kurulunun 22/07/2020 tarih ve 2020/559 sayılı Karar Özeti ['Regarding the transfer of personal data abroad on the basis of Contract No. 108' Summary of the Decision of the Personal Data Protection Board dated 22/07/2020 and numbered 2020/559]," https://www.kvkk.gov.tr/Icerik/6790/2020-559

to the Convention 108's core that mandates the transfer among parties shall not be subject to special authorization of the authorities. Therefore, by eliminating the implementation of the Convention 108 and obliging the data transferring parties to obtain the Board's approval, Turkey has violated its international obligations under the Article 12 of the Convention 108 and Article 2 of the Additional Protocol 181.

In short, while Turkey has adopted the Convention 108's principles and rules in the DPL almost exactly, the compatible implementation of the Convention 108 has collapsed in terms of cross-border data transfers with the Decision of the Board. As a result, the Decision of the Board causes aggressive pressure and disproportionate compliance burden for those who transfer/ host certain data abroad, including both locally operating data controllers and multinational companies.

Comparison of GDPR and the DPL in Terms of Cross-Border Data Transfer

The most significant difference between the GDPR and the DPL can be determined as the cross-border data transfers. While GDPR introduces multiple alternatives facilitating the transfer of personal data, due to cyber security concerns and economic interest of the retention of data, DPL introduces a more controlled and authority-centered structure for the transfer, when the personal data is not transferred with the explicit consent of the data subject.

While the GDPR makes distinction between one-off transfer and ongoing transfers, and considers the nature and purpose of the transfer while deciding the necessary legal protective measure in terms of cross-border transfers, the language of the DPL does not provide such clarity— even though the evaluations to be made in this regard have a significant importance in the proper protection of the data subject. Nevertheless, the practice of the DPL has also been shaped by disregarding such differences, which broadens the role of the Authority in transfers.

On the other hand, while it can be argued that the recently rendered Schrems II Decision—which requires case-by-case analysis to be made by the data protection authorities to ensure that the necessary level of protection is established for each transfer—introduces a stricter regime for cross-border data transfers by increasing the scrutiny over them. It should be underlined that this decision does not imply an approval mechanism to be received by the authorities. Therefore, even this stricter regime would be considered more operable than the DPL, as no direct approval is envisaged and other applicable mechanism is preserved through other safeguards and derogations.

Accordingly, legitimate grounds for cross-border data transfers under both legislation and the current practice in Turkey are summarized in the table provided below:

Legitimate Grounds for Cross-Border Data Transfers	**EU**	**Turkey**	**Turkey- Current Application**
International Agreements	X	X[5]	
Other Laws	X	X[6]	
Adequacy Decision	X	X[7]	
Safeguards			
A Legally Binding and Enforceable Instrument between Public Authorities or Bodies	X		
Binding Corporate Rules	X	X[8]	X[9]
Standard Data Protection Clauses Adopted by the Commission	X		
Standard Data Protection Clauses Adopted by a Supervisory Authority and Approved by the Commission	X		
Code of Conduct	X		
Certification	X		
Contractual Clauses	X		
Administrative Arrangements between Public Authorities or Bodies	X		

[5] Pursuant to Article 90, last paragraph, of the Constitution of the Republic of Turkey, International agreements duly put into effect have the force of law. It also notes that the provisions of international treaties are to be taken as the basis for conflicts which may occur on the ground that there are different provisions on the same topic in law and international treaties relating to fundamental rights and freedoms. Moreover, the 5th paragraph of Article 9 of the DPL specifies that the terms of the international agreement will be reserved.

[6] The last clause of Article 9 of the DPL governs the reservation of the provisions of other laws relating to the transfer of personal data abroad. Thus, the authority on several acts has been given on the international data transfer to the related institutions and organizations. In conclusion, the processes of the aforementioned regulations should be regarded as independent from the ongoing process in the DPL and that the permission of the Board is not required apart from the institutions and organizations authorized for data transfer.

[7] The adequacy decision has not been given by Turkish Data Protection Board till now.

[8] Binding Corporate Rules was introduced by Data Protection Authority on 10 April 2020 based on its announcement. Please see this announcement from the following link (in Turkish): https://www.kvkk.gov.tr/Icerik/6728/YURT-DISI-NA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU

[9] There are no Binding Corporates Rules that have been approved to this date.

Derogations			
Explicit Consent	X	X[10]	X
Conclusion or Performing of a Contract for Data Subject	X		
Conclusion or Performing of a Contract for the Benefits of the Third Party	X		
Public Interest	X		
Legal Claims	X		
Physical or Legal Obstacle Transfers from Public	X		
Transfers from Public Registries	X		
Compelling Legitimate Interests of the Data Controller	X		
Data Controllers located in the transferee and recipient countries give undertakings in writing and the data controller based on the transferee country applies to the board for obtaining permission for the intended data transfer		X[11]	X[12]

As can be seen from the table above, under GDPR there are multiple cross-border data transfer mechanisms that are to be applied in a hierarchical manner in the order shown above. On the other hand, the column indicating the same for Turkey clearly reveals that these alternative data transfer mechanisms under GDPR are not covered in Turkey's data protection legislation. This situation forces cross-border data transfers from Turkey to be held subject to the Board's approval, except for cases where the explicit consent of the data subjects is collected. As explained above, the list of secure countries not yet being published, and the Board's reservation to provide its approval for international data transfers, only reinforces this current situation.

[10] Although explicit consent appears as one of the exceptions in the GDPR application, it is regulated as the main legal basis of data transfer within the scope of DPL. In addition, while the GDPR regulation sets detailed regulations regarding the nature of explicit consent, such as being open and specific, DPL does not contain the same detailed regulations in determining the nature of explicit consent.

[11] Although these commitments are similar to "Standard Data Protection Clauses Adopted by the Commission" and "Standard Data Protection Clauses Adopted by a Supervisory Authority and Approved by the Commission" in the GDPR regulation, they have been evaluated separately as they envisage a different mechanism.

[12] The Board permission has not been granted for any data controller to this date.

Conclusion

The DPL, being adopted from the Directive, falls short of meeting the ever-increasing privacy needs and concerns of individuals, and complicates certain data processing mechanisms, in particular cross-border data transfers.

As the world economy transforms into a data-driven economy, which requires the free flow of data as much as possible to maintain economic relations, all sectors, as well as international trade, have been relying on cross-border data transfers. As the increase in internet usage blurs the borders of international relations and trade, it requires a less restrictive and functioning cross-border transfer mechanism, without compromising on data protection and privacy.

Accordingly, in the short term, the Board shall simplify the "Board Approval" applications in terms of commercial transfers, clarify its scope and framework, and accelerate the finalization process, as this option is the only viable and practicable legal ground in terms of the cross-border data transfers. In this regard, the Board shall conclude applications in a fast and effective manner. Unless the transfer carries a risk of violating privacy of private life in a serious and damaging way, and this risk is high and imminent, the Board shall not reject approval requests.

Moreover, the Board shall determine the list of secure countries who are deemed to be providing adequate level of protection. Political hurdles that are causing this determination to be delayed shall be overcome via mutual dialogues. The Decision of the Board, as explained in detail below, shall also be remedied in a way that ensures the due application and enforcement of Convention 108 and Additional Protocol 181 in domestic law. On the other hand, the Board shall work on introducing other legal bases for cross-border data transfers, which are hierarchical, multilayered, and provide different options depending on the purpose, nature, and intensity of the transfer, as specified in the GDPR.

In line with the strategy set out in the 11th Development Plan and the Annual Program of the Presidency for the Year 2020, Turkey's personal data protection legislation shall be modernized by meeting the highest standards per the data protection law in the world, especially the GDPR. Turkey shall be a party to the modernized Convention 108, and transpose it into domestic law by ratifying it.

Lastly, the Board, which is designated as the competent authority by Turkey for the implementation of the Convention 108 and Additional Protocol 181, shall ensure that the rights of relevant persons are protected in these transfers to contracting states by effectively operating co-operation mechanisms envisaged under these agreements.