ASC law | 20 YIL .YEARS
AKSU ÇALIŞKAN BEYGO ATTORNEY PARTNERSHIP

**24 August 2021**

## PROHIBITION OF TRANSFERRING PERSONAL DATA ABROAD

This information note has been prepared to evaluate the principles of the prohibition of transferring personal data abroad, in line with the purposes of the Law on the Protection of Personal Data (KVKK) numbered 6698, published in the Official Gazette dated 07.04.2016 and numbered 29677.

Paragraph added on 2010 to Constutition *"Everyone has the right to request the protection of his/her personal data. This right includes being informed of, having access to and requesting the correction and deletion of his/ her personal data, and to be informed whether these are used 27 in consistency with envisaged objectives. Personal data can be processed only in cases envisaged by law or by the person's explicit consent. The principles and procedures regarding the protection of personal data shall be laid down in law."* Everyone's right to demand the protection of their personal data is guaranteed as a constitutional right.

In this context, it is envisaged that the procedures and principles regarding the protection of personal data will be regulated by law, while deciding which rights and authorities individuals have over their personal data and in which cases personal data can be processed. As a matter of fact, the procedures and principles regarding the transfer of personal data abroad are regulated in the provisions of article 5, article 6 and article 9 of the KVKK. However, in order to analyze regulation in the most accurate way and to penetrate the spirit of the legal regulations of KVKK on transfer abroad, it is aimed to make a legal review in line with the purposes of the KVKK with this information note.

## I. EXECUTIVE SUMMARY

***(i)*** In principle, it is essential to keep personal data domestically.

***(ii)*** Personal data can only be transferred abroad under limited conditions.

***(iii)*** Personal data cannot be transferred abroad without the explicit consent of the data subject.

***(iv)*** Exceptionally, personal data may be transferred abroad without the explicit consent of the data subject, provided that data controllers in Turkey and in the relevant foreign country undertake in writing to provide adequate protection and that the Board has permission.

***(v)*** Particularly, if the "Binding Company Rules", which are prepared by multinational group companies in accordance with their unique structures, needs and the requirements of the sector in which they operate, and which they undertake to comply with in the transfers of personal data abroad to be made between each other, are approved by the Board, the personal data will be transferred to the group company without seeking the explicit consent of the data subject.

***(vi)*** Transfer of personal data abroad may be partially or completely restricted by Special Laws.

## II. METHODS OF TRANSFERRING PERSONAL DATA ABROAD

The purpose of the KVKK is to determine the rules that must be followed in the processing of personal data, in the protection of personal rights and freedoms, especially in protecting the privacy of private life.

***(i)*** Disciplining the processing of personal data,
***(ii)*** Protection of fundamental rights and freedoms,
***(iii)*** Protection of the individual's right to privacy and information security,
***(iv)*** Regulation of the obligations of natural and legal persons regarding to processing of personal data

Considering the KVKK's aim of "protecting personal rights and freedoms in order to protect the privacy of private life", it has been preferred as a legal policy to keep personal data in the country in order to provide more effective protection on personal data. The biggest reason for this preference is the weakening of the control at the point of protection of personal data in case of transferring personal data abroad. Effective use of this right, which is guaranteed in the Constitution, will be difficult due to weakened control possibilities. For this reason, the transfer of personal data abroad is subject to strict conditions.

### *(i)* Generally

The procedures and principles regarding the transfer of personal data abroad are regulated in Article 9 of the KVKK; The aforementioned article governs the provision that personal data cannot be transferred abroad without the explicit consent of the data subject.

According to this,

I. Provided that the personal data processing conditions specified in the second paragraph of Article 5 of the IKVKK (conditions specified in the third paragraph of Article 6 in terms of sensitive personal data) are met.

   i. In case there is sufficient protection in the foreign country to which the personal data will be transferred (the country with sufficient protection has not yet been determined by the Board), it is possible to transfer the personal data abroad without seeking the explicit consent of the data subject.

   ii. If there is no adequate protection in the foreign country to which personal data will be transferred,

      a. In case the data controllers in Turkey and in the relevant foreign country undertake adequate protection in writing, provided that the permission of the Personal Data Protection Board (Board) is available;

      b. Provided that the rules prepared by the multinational group companies in accordance with their specific structures, needs and the requirements of the sector in which they operate, and which they undertake to comply with in data transfers to be realized between each other, are approved by the Board;

It is possible to transfer personal data abroad without seeking the explicit consent of the data subject.

Based on these articles, the principles regarding the implementation of explicit consent, commitments and binding corporate rules have been regulated by the public announcements of the Board.

### *(ii)* Form and Content of Explicit Consent

Explicit consent; It is “consent on a certain subject, based on information and expressed with free will”. Explicit consent within the framework of the law means that the person gives his/her consent to the processing of his/her data, voluntarily or upon request from the other party. Explicit consent will also enable the data subject to determine the limits, scope, and retention of the data that he/she allows to be processed. In this sense, explicit consent must include the "positive statement of will" of the person giving the consent.

Without prejudice to the regulations in other legislation, it is not necessary to obtain the explicit consent in written form. It also possible to obtain explicit consent through electronic media and call center etc. Here, the burden of proof lies with the data controller.

Within the scope of the definition of explicit consent in Article 3 of the Law, there are 3 elements of explicit consent:

- Relating to a specific subject,
- Consent is based on information,
- Disclosure of free will.

Since explicit consent is a strictly personal right, the given consent can be withdrawn. In this context, since the right to determine the future of personal data belongs to the data subject, the data subject can withdraw the explicit consent given to the data controller at any time. However, since the withdrawal process will have prospective consequences, all activities based on explicit consent should be stopped by the data controller as soon as the withdrawal statement reaches the data controller. In other words, the withdrawal statement becomes effective from the moment it reaches the data controller.

Personal data can be transferred abroad with the explicit consent obtained by complying with the issues explained above. Even in this case, the possibility of withdrawing the explicit consent will cause the risk of data transferred abroad to be transferred back at any time. If the risk materializes, data controllers will have to deal with serious operational difficulties. As a result, the intended results with the transfer abroad will not be achieved.

### *(iii)* Commitments to be given to the Board

Two types of commitments have been prepared by the Board to be used in personal data transfers abroad, both from the data controller to the data controller and from the data controller to the data processor. In the applications to be made to the Board by data controllers,

i. the processing condition on which the personal data transfer is based,
ii. its purpose,
iii. the group or groups of data subject to the transfer,
iv. the administrative and technical measures to be taken by the party to which the transfer will be made,
v. and the retention period

should be detailed in the attachment of the commitment. Otherwise, the commitment application will be rejected by the Board. In addition, the applications made must comply with the procedures and principles that must be followed in the applications to the administrative authorities. The public announcement regarding the issues to be considered in the preparation of the aforementioned commitments was published on the official website of the Board. If the commitment and its annex prepared by the data controller are approved by the Board, they will have fulfilled their obligations to undertake adequate protection set out in subparagraph (b) of the second paragraph of Article 9 of the Law and will be able to transfer personal data abroad.

### *(iv)* Binding Corporate Rules of Multinational Group Companies

Considering that the organizations and business processes of data controllers differ, the Board has established Binding Company Rules (**BCR**) as an alternative method to meet the need to establish appropriate safeguards in order to transfer personal data abroad. In this context, the application form regarding the Binding Company Rules, which can be used in transfers between multinational group companies, and the supplementary document regarding the basic issues to be included in the Binding Company Rules were published and made available to the interested parties on the Board's website.

Accordingly, it is obligatory to include explanations regarding the fulfillment of the following criteria in the BCR application to be made to the Board,

i. The BCR must be legally binding and impose a clear obligation on all group members, including its employees, to comply with the BCR.
ii. The rights of data subject should be clearly recognized in the BCR.
iii. The damages stated in the clause (ğ) of the 11th article of the Law No. 6698 to the data subjects related to the BCR. The possibility of using all legal remedies, including the right to demand redress, should be clearly recognized in BCR.
iv. If the head office of the Group located in Turkey or if the head office of the Group is not in Turkey, a Group member authorized to protect personal data and resident in Turkey, takes the necessary steps to correct the actions of other Group members who are outside the country and are affiliated with the BCR and if the BCR violates it there should be an obligation on the BCR to pay compensation for the material or moral damages that may arise from BCR.
v. The application form must contain a commitment that all BCR members who accept responsibility for the acts of BCR and other members established outside of Turkey, have sufficient assets to compensate for the damages resulting from the BCR's violation.
vi. With BCR; It should be clearly stated that the BCR member who takes the responsibility accepts the burden of proof as to whether the damages claimed by the person concerned are caused by the member abroad.
vii. Comprehensive information should be provided to the data subjects with the BCR regarding their rights regarding the processing of their personal data in the Law No. 6698 and how these rights can be exercised.
viii. The BCR should include an appropriate training program for personnel who have ongoing or regular access to personal data, are involved in data collection, or work in the development of tools used to process personal data.
ix. An internal grievance management process should be established to ensure that any data subject can exercise his or her rights and file a complaint against any BCR member.
x. The requests of the data subjects within the scope of the complaint are concluded as soon as possible and within thirty days at the latest, depending on the nature of the request. In the application form, it should be explained how the data subjects will be informed about the implementation stages of the complaint system.
xi. The BCR should include explanations on how to conduct regular audits and who will carry out this audit in order to ensure compliance with the committed rules.

xii. There should be an appropriate staff structure assigned to ensure and monitor compliance with the BCR for the entire Group. The person or unit that will monitor compliance should be supported by high-level managers.

xiii. The Binding Corporate Rules should include a clear obligation to have all members audited by the Authority, if required, and to agree to abide by the Authority's recommendations on any matter related to these rules.

xiv. The BCR should include the scope of the Rules and a general description of the transfers to enable the Authority to assess whether transactions conducted in third countries are compliant.

xv. The structure and contact details of the group, including each group member, should be clearly stated in the BCR.

xvi. The BCR can be changed/updated, but an obligation should be envisaged to notify all BCR members and the Authority of the changes without delay.

xvii. Security; administrative and technical measures will be taken. In terms of transfers to data processors within the scope of personal data processing activities within the Group, it should be ensured that data processors act in accordance with the technical and administrative measures envisaged by the BCR.

xviii. In case of any personal data breach, it should also include the obligation to notify without delay to the company's headquarters in Turkey or to the BCR members in Turkey authorized for the protection of personal data, and to the relevant data subjects at risk of having their rights and freedoms affected by the breach.

xix. All personal data breaches (including incidents, effects and interventions related to the personal data breach) should be documented and relevant documents should be submitted to the Authority upon request.

xx. If there are provisions in the legislation that a BCR member is obliged to comply with, which prevent the company from fulfilling its obligations under the BCR or significantly affect the implementation of the rules regulated by the BCR, immediately a group member authorized to protect personal data in Turkey must ne notified.

Committed to adequate protection set out in subparagraph (b) of the second paragraph of Article 9 of the Law, if the Board approves the rules prepared by the multinational group companies in accordance with their specific structures, needs and the requirements of the sector in which they operate, and which they undertake to comply with in data transfers abroad to be carried out between each other they will have fulfilled their obligations and will be able to transfer personal data abroad.

## III. CONCLUSION

The procedures and principles regarding the transfer of personal data abroad are subject to strict legal conditions and detailed administrative procedures. For this reason, data controllers need to carry out serious efforts in order to transfer personal data abroad in accordance with the law. Obtaining explicit consent from the data subject in the long run carries great risks such as transferring the personal data transferred abroad back to the country since the data subject has the right to withdraw consent at any time. It is highly likely that the commitments and binding corporate rules, which are prepared meticulously and in a long time, will be found incomplete and rejected by the Board. Only a few data controllers out of thousands of data controllers in Turkey were allowed to transfer personal data abroad based on commitments and binding corporate rules by the Board. Therefore, the tendency of data controllers to domestic personal data transfer options will reduce their legal and operational risks. By providing effective legal protection on the personal data stored in the country, the fundamental rights and freedoms of the citizens will be protected; the domestic data economy will develop; and data controllers will face minimum legal risk due to personal data transfers.

***Please contact us for more detailed information.***


Kemal Tağa

Partner

kemal.taga@aschukuk.com

Emirhan Öncü

Associate

emirhan.oncu@aschukuk.com


*This information note has been prepared as of August 24, 2021 in order to evaluate the transfer of personal data abroad from a legal point of view.*

*The evaluations contained in this information note do not constitute legal advice or legal opinion, and it is not possible to assign any responsibility to Aksu Çalışkan Beygo Attorney Partnership due to these evaluations. It is recommended to seek legal advice regarding your questions and problems within the scope of this information note.*