

# Exemptions under Data Protection Law

August 16 2016 | Contributed by [ELIG, Attorneys-at-Law](#)

## General exemption rule Exemptions to transfer of personal data Comment

The Data Protection Law came into force on April 7 2016. It applies to:

- real persons whose personal data is processed; and
- real persons and legal entities that process such data (wholly or partly) by automatic means or as part of a data filing system by non-automatic means.

Therefore, the general scope of the law is broad and similar to the EU Data Protection Directive (95/46/EC).

### General exemption rule

Article 28 of the Data Protection Law provides exemptions which apply when personal data is processed:

- by real persons in the course of activities that are personal or related to family members living in the same household, provided that the personal data is not shared with third parties and that data security obligations are fulfilled and complied with;
- for research, planning or statistical purposes after being anonymised;
- for artistic, historical, literary or scientific purposes or in the scope of freedom of speech, provided that national defence, national security, public safety, public order, economic safety, privacy or personal rights are not violated and that the data processing does not constitute a crime;
- in the scope of preventive, protective and intelligence activities concerning national defence, national security, public safety, public order or economic safety; or
- in the context of the investigative, prosecution or trial procedures by judicial authorities.

For example, statistics regarding people living in Istanbul who use smartphones where the data has been anonymised by the Statistical Institute could be exempt from the Data Protection Law under the criteria of processing personal data for research, planning or statistical purposes.

Exemptions under the Data Protection Law differ from the EU Data Protection Directive, as they include the criteria of:

- national defence;
- national security;
- public safety; or
- economic safety.

In contrast, activities regarding public safety, defence, the security of member states or state activities in criminal law fall outside the scope of the EU Data Protection Directive.

Under the forthcoming EU General Data Protection Regulation an exemption is given to data processing carried out:

## AUTHORS

[Gönenç Gürkaynak](#)



[İlay Yılmaz](#)



- in the course of an activity that falls outside the scope of EU law;
- by EU member states undertaking activities that fall within the scope of Chapter 2, Title V of the Treaty on the Functioning of the European Union, which regulates the foreign and security policies of member states;
- by a natural person in the course of a personal or household activity;
- by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against threats to public security.

Exemptions to the Data Protection Law, especially those related to the interests of the state, grant broad and ambiguous legal grounds for the processing of personal data. This conflicts with the aim of Article 1 of the law, which states that where the interests of Turkey or the data subject will not be seriously undermined, personal data may be transferred abroad if authorised by the Protection of Personal Data Board. However, the provision is ambiguous and does not:

- specify criteria for assessing how the transfer of data abroad could seriously harm the interests of Turkey or the relevant party;
- define precisely the circumstances in which the transfer of data abroad will be subject to the board's permission; or
- designate an authority or specify which party will decide whether permission is required regarding the transfer of data abroad.

The Data Protection Law does not specify the terms or conditions referred to therein. Therefore, it differs from the EU Data Protection Directive in that regard.

Although national defence, national security and public safety could be seen as providing legitimate grounds for exemptions under the Data Protection Law, this point should be clarified in detail and the limitations prescribed. If the scope of exemptions remains broad, it could result in violations of Article 20 of the Constitution and Constitutional Court decisions where privacy and the protection of personal data are protected as basic human rights. In order to prevent such violations, the scope of exemptions to the Data Protection Law should be amended and defined more specifically in line with EU data protection law. EU data protection law provides exemptions from the EU Data Protection Directive regarding:

- national security and defence;
- the prevention, investigation, detection and prosecution of criminal offences; and
- the protection of data subjects and the rights and freedom of others.

For similar reasons, under these exemptions the following obligations can be bypassed:

- the obligation to inform the data subject about the processing of his or her personal data;
- the obligation to reveal certain data processing operations to the data subject;
- the right of the data subject to access his or her data;
- the right of access to statistical or research data; and
- the obligation to ensure basic principles of good data management.

Exemptions regulated under the Data Protection Law should focus on specific rights and not be used as a general exemption rule. For example, personal data may be exempted from non-disclosure provisions if the disclosure aims to protect national security. However, national security should not be the legal basis of a general exemption in data protection legislation.

### **Exemptions to transfer of personal data**

The Data Protection Law makes a distinction between the transfer of personal data in Turkey and abroad. Accordingly, personal data cannot be transferred without the explicit consent of the data subject. However, if the data subject's explicit consent is not required to process personal data, as set out in Article 5 of the Data Protection Law, consent for the transfer of data abroad is not required.

Article 5 sets out the following conditions for which a data subject's explicit consent is not required

to process personal data:

- data processing that is explicitly foreseen by law;
- data processing that is required to protect the interests or integrity of the data subject or of another person where the data subject is physically or legally incapable of giving his or her consent;
- the processing of personal data of parties to a contract on the condition that it directly relates to the execution or performance of a contract;
- processing that is required to comply with a legal obligation to which the data controller is subject;
- data that is made publicly available by the data subject;
- data processing required to establish, exercise or defend a legal claim; and
- data processing required under the legitimate interests of the data controller, as long as the data subject's rights are unharmed.

If the processing of personal data does not require the explicit consent of the data subject, data can be transferred abroad without the explicit consent of the data subject provided that:

- the destination country has an adequate level of data protection, as determined by the Protection of Personal Data Board; or
- data controllers in Turkey provide a written declaration that there is an adequate level of data protection in the relevant foreign country.

For example, a company located in Turkey may transfer personal data to an affiliate company overseas for billing purposes without obtaining the data subject's consent, as the consent for data processing is not required for the performance of a contract if the affiliate company is located in a country that the Protection of Personal Data Board deems to be trustworthy.

As regards sensitive information, where data can be processed without the explicit consent of the data subject (eg, where stipulated by law or in the case of health data for the purpose of protecting public health), sensitive data may be transferred abroad without the explicit consent of the data subject provided that:

- the relevant country has an adequate level of data protection, as determined by the Protection of Personal Data Board; or
- data controllers in Turkey provide a written declaration that they have ensured an adequate level of protection in the relevant foreign country.

Article 9(5) of the Data Protection Law states that where the interests of Turkey or the data subject will be seriously undermined, personal data may be transferred abroad with authorisation from the board. This provision was added to the law at the end of the enactment process.

However, Article 9(5) is ambiguous and does not:

- specify criteria to assess or determine how the transfer of data abroad could harm the interests of Turkey or the data subject;
- define precisely circumstances in which the transfer of data abroad will be subject to permission from the Protection of Personal Data Board; or
- designate an authority or specify which party will decide whether permission is required regarding the transfer of data abroad.

As there is no specific criteria regarding the conditions for transferring data abroad that require the Protection of Personal Data Board's permission, the potential consequences of Article 9(5) are unpredictable. A data controller or processor may not be in a position to determine whether the transfer of data abroad could harm the interests of Turkey or the relevant party. Considering Article 9(5) as a general requirement for the transfer of data abroad would be counter to the aims of the Data Protection Law. Therefore, this provision should be considered an exceptional option for sensitive issues.

A considerable amount of personal data is being transferred across borders every day in the

European Union by businesses, public authorities and individuals. Conflicting data protection rules in different countries could disrupt the international exchange of data. Individuals could also be hesitant to transfer personal data abroad if they are uncertain about the level of data protection provided in other countries.

## **Comment**

Although the Data Protection Law was based on the EU Data Protection Directive, there are a number of issues that must be examined and clarified to avoid the potential conflicts cited in this update. The exemption to the Data Protection Law under Article 28(1)(c) provides excessive rights through the broad exemptions granted to government authorities. For example, if personal data is processed by public institutions and organisations "which are authorized by law within the scope of their preventive, protective and intelligence activities for national defence, national security, public safety, public order or economic safety", the Data Protection Law is not applicable. However, data may be also processed in a way that it is unrelated to the legal grounds of "national defence, national security, public safety, public order or economic safety". Therefore, the provision exempts certain government authorities from complying with data protection measures. Further, Article 9(5) is an ambiguous provision which sets no criteria to evaluate or determine how the interests of Turkey or relevant persons could be damaged and fails to clarify the circumstances in which the transfer of data abroad will be subject to permission from the Protection of Personal Data Board or specify which party will decide whether permission is required regarding the transfer of data abroad.

*For further information on this topic please contact [Gönenç Gürkaynak](#) or [İlay Yılmaz](#) at ELIG, Attorneys at Law by telephone (+90 212 327 17 24) or email ([gonenc.gurkaynak@elig.com](mailto:gonenc.gurkaynak@elig.com) or [ilay.yilmaz@elig.com](mailto:ilay.yilmaz@elig.com)). The ELIG, Attorneys-at-Law website can be accessed at [www.elig.com](http://www.elig.com).*

---

The materials contained on this website are for general information purposes only and are subject to the [disclaimer](#).