

## PERSONAL DATA PROTECTION LAW

### Decision Summaries of the Month & News

#### Deadline for VERBIS Registration Has Been Extended

**Decision No:** 2019/265

**Decision Date:** 03/09/2019

**Subject:** Decision of the Board regarding the extension of the deadline for VERBIS Registration.

As a result of the evaluation of the requests conveyed to the Personal Data Protection Authority by several organizations for the extension of the registration deadlines to the Data Controllers' Registry, the deadline determined for fulfilling the registration obligation to the Registry for the real and legal person data officers with more than 50 employees or a total annual financial balance of more than 25 million TL and real and legal person data officers residing abroad has been extended until 31.12.2019.

#### The European Court of Justice has ruled that Google only needs to comply with the right to be forgotten within the European Union

**Decision No:** C-507/17

**Decision Date:** 24/09/2019

**Subject:** Decision about whether search engine operator Google should block non-European pages within the scope of "right to be forgotten".

In the case, the French Data Protection Authority (Commission Nationale de L'informatique et des Libertés - CNIL) submitted a claim to the European Court of Justice (ECJ) that, Google has to be punished since it is only deleting the results of the data owners' search results only in the European Union domain names.

As a result of the complaint of the Authority, the following provision has been established by the Court:

1. In the application under which the complaint is lodged, an examination of the fact that this may be considered in the regional context under Article 10 of Directive 95/46 and Article 10, 11 and 13 of Regulation 2016/679, which is based on Article 16 of the TFEU, but what is to be understood from the regional context and that it is true that

the removal of all search results about the person under the right to be forgotten will fully meet the relevant provisions,

2. However, it is stated that the internet is a global network with no boundaries, and that search engines provide information and links in the list of results displayed after a search based on the presence of the individual's name everywhere. In a globalized world, it should be emphasized that although all countries except the Union have different approaches to the to the "right to be forgotten" and not all of them recognize this right, although they have access to a connection with immediate and significant impact on the person referring to person within and outside the European Union,
3. Moreover, protection of personal data is not an absolute right, but should be considered in relation to its function in society and balanced against other fundamental rights in accordance with the principle of proportionality. In addition, the perspective on the balance

between the right to privacy and the protection of personal data and the freedom of information of internet users has changed significantly around the world,

4. In the light of the laws of the European Union, currently the search engine operator does not have any obligation to delete the his/her data who requested it from all its domain names,
5. Furthermore, the decisions made in the data protection laws of the European Union are applied directly in all member states and therefore are not only in a single member state of the Union; in all member states of the Union, the right to be forgotten must be observed and in the results of searches made with the name of the person having data from one of the member countries, protection of the person having data effectively or severely deterring and seriously discourage an internet user conducting a search should be provided,
6. Nevertheless, even within the Union member states on whether freedom of information, especially in the context of journalism or artistic or literary expressions, would constitute an exception as a result of the joint consideration of the rights of the public in accessing information and the rights of privacy and protection of the personal data of the data subject, there is a difference and therefore national supervisors need to reach a compromise and take a binding decision for all member states.

There are important points to be addressed in this decision. Namely;

1. The Court rules that the right to be forgotten is not an absolute right and should therefore be considered all together with

other fundamental rights and proportionality,

2. The search engines should delete links containing embarrassing or outdated information belonging to the requestor, if is requested by the data owner,
3. However, this shall not be extended to other countries other than the member states of the European Union which do not have to comply with the laws of the Union.

### **Youtube Will Pay a Penalty of 170 Million Dollars For Breach of Coppa Rules**

Youtube and Google, to which it is affiliated, have compromised with the Federal Trade Commission and New York attorneys as a result of the investigation on the grounds that Youtube collected the children's data through the channels for children without their parents' permission by violating Children's Online Privacy Protection Act ("COPPA"). As a result of the compromise, Youtube will pay a record-breaking penalty of \$ 170 million to FTC and New York State. This the highest amount of penalty FTC receives from an institution after the adoption of the COPPA.

In addition to fines that Youtube and Google were imposed, it was also agreed with FTC and attorneys that Youtube

- shall develop a system in which the content for children can be defined,
- shall notify channel owners that they are subject to COPPA obligations,
- shall provide annual COPPA compliance training to Youtube employees associated with channel owners,
- shall provide information before collecting children's personal data and obtain

veritable explicit consent from their families.

### **Polish DPA imposes €645,000 fine for Personal Data Violation**

The Polish Personal Data Protection Office imposed a fine of an amount higher than PLN 2.8 million (ca. 645,000 euros) on Morele.net for company's improper organisational and technical measures to protect personal data. These measures were the lack of appropriate intervention procedures in the event of unusual network traffic. The said lack had risks like as to reach the personal data of approximately 2.2 million people such as name, surname, phone number, e-mail and delivery addresses in the wrong hands, such as identity theft. When penalizing such actions, as the company's steps to end the breach, good cooperation with the supervisor, and the fact that the company had not previously violated the personal data protection law were taken into consideration by The Polish Office for the Protection of Personal Data.

### **Türkiye İş Bankası A.Ş. – Data Breach Notification**

According to the data breach notification made by İş Bankası A.Ş., it was determined that within the scope of data leak prevention works carried out at the bank, a branch employee forwarded e-mails containing the Risk Center queries in the attachment to non-bank users; in the preliminary examination, it was determined that the person had transferred the reports he had obtained by misusing his duties to third parties for money. The said breach was published on the Authority's website on 12.09.2019 and the

investigation is continuing regarding this issue.

### **FER Gayrimenkul Geliştirme ve İnş. A.Ş. – Data Breach Notification**

According to the data breach notification by FER Gayrimenkul Ticaret ve San. A.Ş.; a cyber-attack took place by entering to the company logs; as a result of the cyber-attack, nearly 1200 employees' and customers' identity, communication and financial information were retrieved. The breach was published on the Authority's website on 12.09.2019 and the investigation is continuing regarding this issue.

### **Furtrans Denizcilik Ticaret ve San. A.Ş. – Data Breach Notification**

According to the data breach notification made by Furtrans Denizcilik Ticaret ve San. A.Ş., access to the company data was denied by a cyber-attack to

company systems; as a result of the attack, about 500 employees, user, subscriber / member, student customers' identity, communication, location, personal, legal transaction, customer transaction, physical space security, transaction security, risk management, finance, professional experience, visual and audio record information, health information and biometric data were copied and passed on to the third parties. The breach was published on the Authority's website on 18.09.2019 and the investigation is continuing regarding this issue.

### **Zynga Game Ireland Limited - Data Breach Notification**

According to the data breach notification made by Zynga Game Ireland Limited; the company's system was illegally accessed on 31.08.2019; as a result, there has been a breach of the identity, communication and location information of 34,000 Turkish citizens. The breach was published

on the Authority's website on 26.09.2019 and the investigation is continuing regarding this issue.

### **Gardrops Elektronik Hizmetler ve Ticaret A.Ş. - Data Breach Notification**

According to the data breach notification made by Gardrops Elektronik Hizmetler ve Ticaret A.Ş.; as a result of the correspondence with the person who claimed to have illegally accessed the company's website on 13.09.2019, it was determined that 25 persons' names, surnames, e-mail addresses and encrypted user account passwords were accessed, and as a result of technical investigations, a maximum of 257,000 users may have been affected by the breach. The breach was published on the Authority's website on 26.09.2019 and the investigation is continuing regarding this issue.



# INFORMATION GUIDE

## PERSONAL DATA PROTECTION LAW

### Featured Topics

#### **OBLIGATION OF VERBIS REGISTRATION AND DCR APPOINTMENT FOR DATA CONTROLLERS RESIDENT ABROAD**

In the event that some or all of the personal data is transferred to the founder / partner foreign company residing abroad and **the foreign company residing abroad uses this data for its own purposes**, there is an obligation to register at the Data Controllers' Registry Information System (hereinafter referred to as "VERBIS") for the foreign company. These transfers, in general, consist of recordings of all or part of the data of the employees, suppliers and customers of the legal entity in Turkey **to a registration system which is provided and managed by foreign partner**. However, keeping only the personal data in a registration system by the foreign partner does not constitute a registration obligation of VERBIS and the foreign partner is required to use this data for its own purposes.



In accordance with this explanation; the legal entity resident abroad or with a partner company's founder identity in Turkey has to register VERBIS **by means of a Data Controller Representative**.

This obligation of registration is based on the reciprocity and has come out with the same purpose of the provision regulated in the Art. 3 of GDPR as follows "*This Regulation also applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union.*"

Here are the most important points to be noted:

1. Once the data controller resident abroad processes the data of a Turkish resident or a Turkish citizen, legal liability comes out for the data controller.
2. Data controller residing abroad has to submit a declaration to the registry by fulfilling VERBIS registration by 31.12.2019 being subject to KVKK without providing any other conditions.
3. If the company resident abroad is processing data through its subsidiary or affiliated company, both companies are obliged to register at VERBIS separately. (VERBIS registration is not obligatory if the domestic company does not have one of the conditions stipulated in the Board Decision 2018/88.)
4. The domestic company, which is affiliated with the company resident abroad, has no responsibility for not fulfilling the registration obligation of the company resident abroad.
5. The data controller resident abroad has to appoint a DCR who is a resident in Turkey to make VERBIS registration according to the Article 11 of the Regulation on the Data Controllers' Registry.
6. A DCR appointment decision with a decision number shall be delivered to the Board with a wet signature and apostille.
7. The appointment decision shall issue the following authorizations:
  - a) Notification or acceptance of notifications or correspondence made by the Authority on behalf of the data controller,
  - b) Forwarding the requests of the Authority directed to the data controller to the data controller and forwarding the response of the data controller to the Authority,
  - c) In case, no other basis has been determined by the Board; receiving applications of the relevant persons on behalf of the data controller and forwarding them to the data controller, in accordance with the first paragraph of the Article 13,
  - d) In case, no other basis has been determined by the Board; forwarding the response of the data controller to the relevant persons, in accordance with the third paragraph of the Article 13,
  - e) Carrying out the works and transactions related to the VERBIS on behalf of the data controller.



**YOUR TIME IS RUNNING OUT !**

**HAVE YOU COMPLETED YOUR VERBIS REGISTRATION YET?**

[Click Here](#)

# LEGISLATION ANALYSIS

## PERSONAL DATA PROTECTION LAW (KVKK)

### Analysis: Article-9/5 Transfer of Personal Data Abroad

#### Transfer of Personal Data Abroad

##### Article 9 / 5

Transfer of personal data abroad should be carried out in a different way from the normal course in some special cases, without prejudice to the provisions of the international convention. A different method is provided in the law to transfer these data abroad in special cases where contrary to Turkey's or the interest of the person concerned. Information that Turkey possess which are regarded as secrets, information on the property rights of persons, health data obtained for the purpose of mapping gene countries can be examples for the topics concerning Turkey or the interest of the relevant persons. As it is seen, since these data and the scope of the interest are not limited, an assessment should be made according to concrete cases.

If the real or legal person to transfer the data is in the opinion that the data transfer activities will harm the interest of Turkey or the relevant person concerned, then data transfer shall be followed by following the way specified in the Art. 9 of KVKK. The steps to be followed will vary depending on whether the country of transfer is a safe country or not:

**First Possibility :** If the requirements in Art. 5/2 or Art. 6/3 of KVKK are met and the country to which data transfer is counted among the safe countries, permission for transfer is requested from the Board. The Board shall take the opinion of a public institution and, if necessary, the Ministry of Foreign Affairs and decide on the transfer of data.

**Second Possibility:** If the requirements of Art. 5/2 or Art. 6/3 of KVKK are met and the country where the data transfer is not counted among the safe countries, by taking a commitment from the person to whom the data will be transferred to ensure the security of the data; permission is requested from the Board within the scope of this commitment. The Board evaluates the commitment and the opinion received from the relevant public institution and, if necessary the Ministry of Foreign Affairs together and decides on the data transfer..



*(5) In cases where interest of Turkey or the data subject will seriously be harmed,*

*personal data, without prejudice to the provisions of international agreements, may only be transferred abroad upon the permission to be given by the Board after receiving the opinions*

*of related public institutions and organizations.*

***Particular attention should be paid here that in cases where the explicit consent of the person concerned or the country to which the data is to be transferred is a safe country in subjects not covered by Art. 9/5 of KVKK, data can be transferred without any further steps; but, in cases covered by Art. 9/5, the explicit consent of the person concerned is not a valid method of data transfer and Board's permission shall be obtained even if the country to be transferred is a safe country.***

**In addition, since the Board has not yet announced the list of safe countries, only the method given under the title "second possibility" shall be applied until the list of safe countries is announced.**

### **Notification !**

Contents provided on this article serve to informative purpose only. The article is confidential and property of CottGroup® and all of its affiliated legal entities. Quoting any of the contents of this notification without credit being given to the source is strictly prohibited. Regardless of having all the precautions and importance is put in the preparation of this article, CottGroup® and member companies cannot be held liable of the application or interpretation of the information provided. It is strictly advised to consult a professional for the application of the above-mentioned subject. Prior to taking any action in regards the above.

Please consult your client representative if you are a customer of CottGroup® or consult to a relevant party.