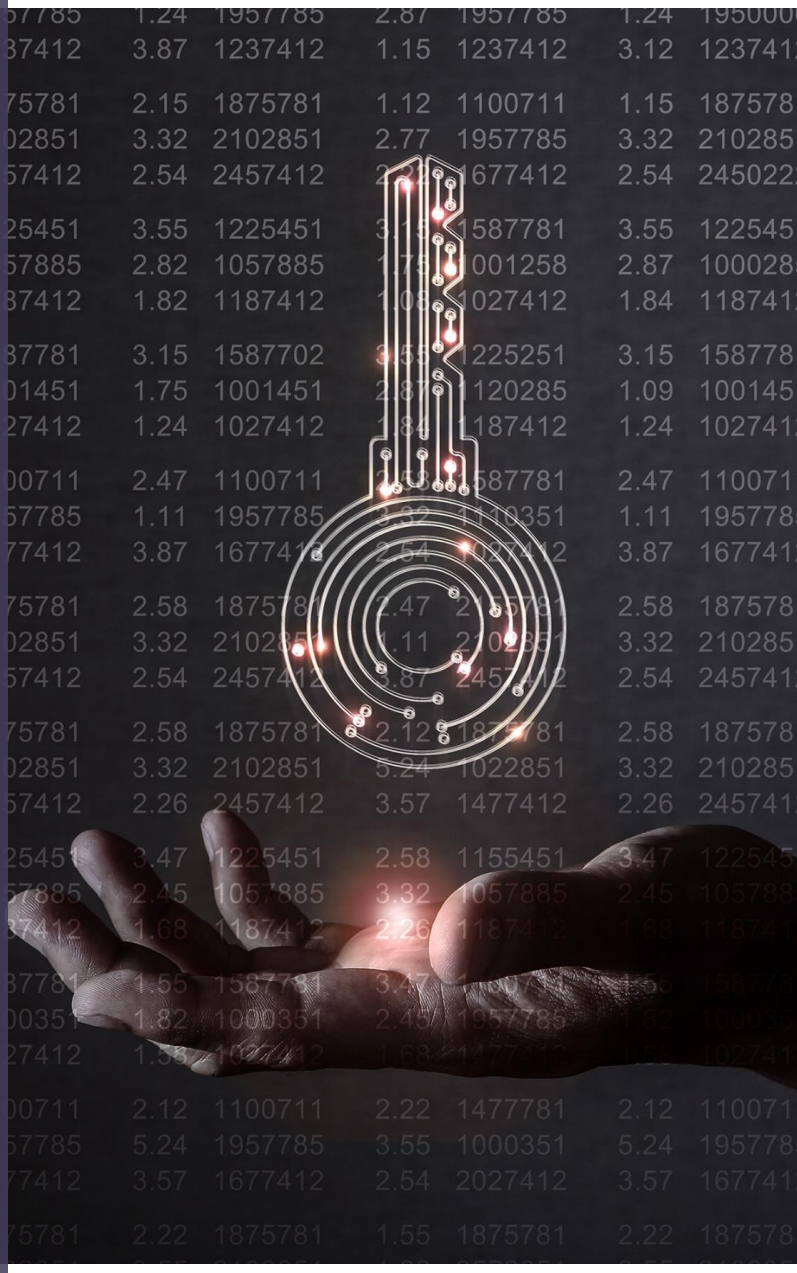
CottGroup®
Holistic Business Services

VeriSistem
a CottGroup® company



KVKK & GDPR NEWSLETTER

NOVEMBER 2020

DECISION SUMMARIES OF THE MONTH AND NEWS

Board Decision About an Association for Sending Short Messages to the Data Subject for Advertising Purposes Without Obtaining Explicit Consent

Decision No: 2020/691 **Date of Decision**: 10.09.2020

Abstract: Board Decision about an association for processing the mobile number of the data subject to send short text messages for advertising purposes without its explicit consent

According to the complaint conveyed to the Turkish Data Protection Authority, an association sent short text messages to the data subject without obtaining its explicit consent; upon that the data subject applied to the association and requested information; however, the association did not give any response to the data subject within the legal period of 30 days. As a result, the data subject applied to the Authority and requested all irregularities to be revealed and the necessary sanctions to be applied.

Based on the information request made by the Authority, it is stated in the response letter sent by the association that;

- They received the application of the data subject; but the answer could not be sent to him due to an administrative problem;
- After the application of the data subject, the mobile phone number in question was immediately rendered inactive not to send any messages;
- They could not determine whether they have the explicit consent of the data subject for sending short text messages;
- There is no information processed by the association other than the mobile phone number of the data subject and the information in question was possibly obtained as a result of a donation made through this mobile phone number;
- The short text message in question was sent to the data subject by the association.

As a result of its examination, the Board has concluded as in the following,

- In the absence of compliance with the applicable law, other than explicit consent specified in Article 5 of the Law, personal data can be processed with the explicit consent of the data subject;
- Even if there are cases of compliance with the law, it is necessary to act in accordance with the basic principles stated in Article 4 of the Law in all cases and conditions; however, in the present case, the reason for the processing of the mobile phone number of the data subject, which is the personal data of the person, could not be proved and there was no clear statement regarding this issue;

- The statement made by the Association as "*it is highly probable that the data subject made a donation before through short message*" is not a statement based on legal grounds, nor can it be accepted as a valid statement;
- It was acknowledged that the said short message was sent by the association to the data subject without explicit consent;
- In the incident subject to the complaint, the reason why the association did not respond to the request to obtain information was stated as an administrative problem was not explanatory and that it was clearly contrary to the Law;
- The data processed unlawfully from the beginning should be deleted immediately and the unlawfulness should be eliminated,
- With the assessment that in terms of the incident subject to the complaint, blacklisting/making the mobile phone number passive does not mean that the personal data processed unlawfully has been deleted, that the personal data are kept without any legal basis, the mobile phone number in question should be destructed in order to prevent the unlawfulness,
- It has been decided that an administrative fine to be imposed to the association,
- The association to be instructed to take care to respond to the applications of the data subject within the legal period,
- The association to be instructed to destruct the mobile phone number of the data subject which has already been obtained unlawfully.

UPİ Trans Dış Ticaret A.Ş. - Data Breach Notification

With the data breach notification made by UPI Trans Dış Ticaret A.Ş., it was reported to the Authority that the company's servers were encrypted as a result of a cyber-attack which was performed on 29.10.2020 at 10:00, and it was detected on the same day. It was stated that the personal data affected by the breach are; identity, communication, employee information, legal transaction, customer transaction, finance, marketing data with visual and audio records; sensitive personal data affected by the breach are data on philosophical belief, religion, sect and other beliefs, health information, information about criminal conviction for security measures. It was stated that the estimated number of people is 50 such as employees, users, customers and potential customers and people who have not yet been identified are affected by the breach, but the number of people could not be determined exactly.

The aforementioned data breach was published on the website of the Authority on 06.11.2020 and the investigation on the subject still continues.

Kale Holding A.Ş. and Group Companies - Data Breach Notification

Having the title of data controller, Kale Holding A.Ş. and its group companies Bodur Gayrimenkul Geliştirme A.Ş, Kale Nakliyat Seyahat ve Turizm A.Ş., Kalekim Kimyevi Maddeler Sanayi ve Ticaret A.Ş., Kalemaden Endüstriyel Hammaddeler Sanayi ve Ticaret A.Ş., Kaleseramik Çanakkale Kalebodur Seramik Sanayi A.Ş. stated with the data breach notification that the data breach occurred on 04.11.2020 in the form of encryption of some databases on the server. Personal data affected by the breach, the number of persons and records, and the groups of persons affected by the breach have not been determined yet. It was stated that the investigation by the data controllers about the data breach continues.

The aforementioned data breach was published on the website of the Authority on 12.11.2020 and the investigation on the subject still continues.

Çizgi Telekomünikasyon A.Ş. - Data Breach Notification

With the data breach notification made by Çizgi Telekomünikasyon A.Ş., the employee who came to the company for the weekend shift on November 7, 2020, found a message on the server desktop when he was connected to the server remotely to perform routine checks. As a result of the routine check, it was reported to the Authority on the same day that some malware was found on the servers of the company where customer information was stored.

Information such as Turkish ID number, name and surname, e-mail and home addresses, customer transaction details (such as credit card information), the services purchased by the customer and the date-time information subject to transactions related to these services may be affected by the breach. It has been stated that the number of persons and records affected by this breach has not been determined yet; and the investigation still continues.

The aforementioned data breach was published on the website of the Authority on November 12, 2020 and the investigation on the issue still continues.

EDPB Has Made Its Initial Decision Regarding Dispute Resolution Between Supervisory Authorities of Member Countries within the Scope of Article 65 of GDPR

Article 65 of the GDPR relates to the resolution of disputes by a binding decision by the EDPB when a dispute arises between the data protection authorities of countries and has been applied for the first time.

In January 2019, Twitter International filed a notification of data breach to the Irish Data Protection Authority. Upon that, the Irish Data Protection Authority, as the Lead Supervisory Authority, has made a draft decision regarding Twitter International and has forwarded this decision to the concerned supervisory authorities.

Thereupon, the concerned supervisory authorities have submitted their reasoned objections to the Irish Authority regarding the evaluation of Twitter International as data officer and the amount of penalty determined. The reasoned objections were not accepted by the Irish authority as the Lead Supervisory Authority. After that, the EDPB was applied by means of dispute resolution.

After its assessment, the EDPB made its binding decision and reported it to the Irish Authority. Thereupon, the Irish Authority will make the final decision by observing the EDPB decision within 1 month from the notification of the decision and will notify the data controller. It is expected that this decision will be published on the EDPB website after notification of the decision to the data controller.

Italian Data Protection Authority Fines Vodafone

Customers have made hundreds of complaints and warnings for unwanted phone calls to Vodafone made by the company or the company's sales network to promote telephone and internet services. As a result, the Italian Authority stated that it has initiated a judicial process against Vodafone.

The most interesting finding identified in the investigation is the use of fake phone numbers and the numbers not registered with the ROC (i.e. the National Consolidated Registry of Communication Operators) to make marketing calls. The Authority stated that additional violations may occur related to the processing of contact lists purchased from external providers.

In addition, The Authority has instructed Vodafone to set up systems that will show that processing for telemarketing purposes complies with the permit requirements. However, the Authority prohibits data processing for marketing or commercial purposes where user details are obtained from third parties without their free, private and informed data disclosure consent. In addition, the authority imposed a fine of over 12.250.000 EUR to Vodafone.

Spanish Data Protection Authority Fines Telefónica Móviles España

In the incident where the plaintiff stated that it contacted the Data Controller due to an error in the invoicing process and the Data Controller stated that the processing activity belongs to the bank, it was determined by the Spanish Data Protection Authority that the defendant processed the plaintiff's data unlawfully, and Telefónica was imposed a fined of 75.000 EUR due to violation of Article 6/1 of the GDPR.

Norwegian Data Protection Authority Fines Østfold HF Hospital

Stating that the data breach started as a result of the exclusion of the reports stored in Østfold HF Hospital between the period 2013-2019 from the safe area and registering the patient records, the Authority stated that access control was not made to the folders where the extracts were stored, access to personal information was provided to 118 employees in the hospital and most of them did not have a formal and justified need for this access. The Authority also realized that the report abstracts were kept even though the need for retention disappeared, and imposed a fine of 750.000 NOK to the hospital.

LEGISLATION ANALYSIS

The Principle of Purpose Limitation in the Scope of Article 4 of KVKK and Article 5 of GDPR

Article 4 of KVKK – General Principles

...

(2) The following principles shall be complied within the processing of personal data:

...

c) Being processed for specific, explicit and legitimate purposes.

...

***

Article 5 of GDPR - Principles relating to processing of personal data

1. Personal data shall be:

...

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; … ('purpose limitation');

...

***

There are principles determined on the basis of the rules regarding the protection of personal data. These principles constitute the framework that surrounds all rules in the protection of personal data and affects each activity of the addressees of the rules. It is a general obligation to act in accordance with the principles, and the violation of these principles is subject to penalties regarding the relevant rules. The purpose limitation is one of these principles that are included in the Article 4 of KVKK and Article 5 of GDPR.

According to the principle of purpose limitation, data controllers are required to process data only for specific, legitimate and explicit purposes. Data controllers should be clear about their data processing activities and their operations on data should be in line with the expectations of the data subject. In this respect, data controllers should clearly state their purposes for data processing both in their internal records and when providing information to the data subject.

The principle of purpose limitation is highly related with principles of fairness, lawfulness and accountability. Being specific and clear for what purposes the data is processed ensures that the conditions of these other principles are also established, on the other hand, not using it for a limited purpose creates incompatibility with the mentioned principles.

Accordingly, data controllers shall:

- Be clear about why and for what purposes they collect the personal data in question,
- Prepare and keep the necessary documentation in which the objectives are explicitly stated,
- Be transparent to the data subjects regarding the purposes,
- If a purpose other than the one from which the data was obtained emerges, ensure that this second purpose is lawful.

It is possible that the purpose of collection may differ over time. For example, the initial purpose for which data from the data subject is collected and used may end and a new purpose may arise. In this case, if the new purpose is compatible with the initial purpose, a new legal reason assessment is not required and the legal justification of the initial purpose remains valid for the new purpose. On the other hand, if the new purpose is not compatible with the initial purpose, then the compatibility assessment for the new purpose should be carried out again for KVKK or GDPR, for example, the legal reason should be specified again. However, it should not be forgotten that the obligation to inform the data for the new additional purposes continues in any case.

Compatibility assessment between purposes should be based on the present case. Besides, the following points are indicative:

- The relation between the initial purpose and the new purpose,
- The context in which personal data are collected at the beginning, especially the relation between the data subject and the data controller, and the reasonable expectations of the data subjects,
- The nature of personal data, especially whether they are sensitive or not,
- The consequences of data processing for the new purpose and likely to create for the data subjects,
- Availability of appropriate and necessary measures such as encryption.

As a general rule, if the new purpose is different from the initial purpose or if it falls outside the expectations of the data subjects or if it will have an unfair effect on the data subjects, it is likely to be incompatible with the initial purpose.

Rabia Dağcı | Legal Consultant | Attorney | CIPP/E

Prepared By

Ece Melis Erkoçak

Hazal Özçelik

Kerem Akdağ

Kübra Özkahraman

Livanur Sever

Onur İzli

Rabia Dağcı

Şeyma Kaplan

Şule Özcan

Follow Us on Social Media...