

KVKK & GDPR

NEWSLETTER

Monthly Newsletter

JULY 2022



- Decision Summaries
- News
- KVKK-GDPR Reviews

01

Summary of the Decision Numbered 2019/198 Regarding the “Notification of the Data Subject that Unlawful Personal Data Has Been Processed by the Data Controller Within the Scope of a Loyalty Program”

In the complaint petition submitted to the Authority, it was stated that a special discount was applied to the “Sadakat Kart” (Loyalty Card) for some products sold in the store of the Data Controller, so that special discounts were applied conditionally, the personal data of the customer was requested for membership in said loyalty program and card supply, and explicit consent was imposed as a condition.

As a result of the investigation carried out by the Turkish DPA, it is determined that the opportunity to shop at the stores of the data controller for the persons who do not want to be included in the “Loyalty Card Program” and/or who do not want to give explicit consent within the “Loyalty Card Program” is not abolished and sales are continued at non-discounted prices to the customers who are not members of the “Loyalty Program” and offering products/services at a discount with additional benefits within the scope of the loyalty program does not mean that express consent is imposed as a condition.

Based on these evaluations, the Turkish DPA has decided that there is no action to be taken against the Data Controller within the scope of the law.

You can find the detail of the Decision [here](#).

02

Summary of the Decision Numbered 2021/1258 Regarding Unlawful Processing of the Personal Data of the Data Subject by the Data Controller Company Whose Employment Contract Has Ended

In the complaint petition submitted to the Authority, it was stated that worked at the data controller company at a certain time, when the data subject wants to apply for the data controller company for personal data, the data controller hasn't got an application form and the means of application were not notified, the obligation to inform is not fulfilled in accordance with the law, sensitive personal data of data subject was processed without his/her explicit consent, the entrance to the data controller company is made with fingerprint and face scanning system, different companies of the group have branches abroad, and when the data subject visited the abroad branch, his personal data had been transferred abroad without his explicit consent, adequate technical and administrative security measures have not been taken for his/her personal data, there is no privacy policy on the company's website.

As a result of the investigation carried out by the Authority, it is determined that the clarification text added as an article to the employment contract of the data subject is a mixed text, which also has the nature of an explicit consent text, that the clarification text does not contain the minimum factors processing biometric data based on the condition of explicit consent is unlawful.

Based on these evaluations, the Authority has decided to impose an 125.000,00 TRY administrative fine on the data controller.

You can find the detail of the Decision [here](#).

03

Summary of the Decision Numbered 2021/1262 Regarding “the Personal Data Processing of the Bank Data of the Data Subject by An Insurance Company”

In the complaint petition submitted to the Authority, it is stated that although the Data Subject has not shared the bank information of his/hers with the insurance company who is the Data Controller, this information have been processed unlawfully by the insurance company, the data subject has requested information regarding the subject from the data controller through his/her representative, and also requested the deletion or destruction of his personal data, yet his application has been left unanswered.

As a result of the investigation carried out by the Authority, it is determined that in the concrete case, in spite of the fact that the application submitted by the data subject to the data controller through his/her representative, which has been received by the data controller, was not answered due to lack of proxy included special authorization, since there is no regulation within the scope of KVKK regarding the need for a special power of attorney for the application made by the data subject through their representatives, special authority should not be sought by the data controller.

Based on these evaluations, the Turkish DPA has decided that there is no action hasn't been taken against the data controller within the scope of the law.

You can find the detail of the Decision [here](#).

04

Summary of the Decision Numbered 2021/1303 Regarding the “Processing of the Data of the Data Subject and Establishment of a Blacklist Program that Ensures the Sharing of This Data Between Car Rental Companies by Car Rental Program Software and Vendor Companies.”

In the complaint petition submitted to the Authority, it is stated that the notified data controllers are automobile renting software manufacturers or vendors, the automobile renting companies using these software record all the data they obtain about their customers through these software, and in this context, other companies using the same software can also see the personal data of the relevant customers from the blacklist pool in the application without their consent, and so that the data is disclosed to other users using this software, they are enrolled to the blacklist by means of this software without the consent of the customers, and thus their personal data is shared with other users using this software. As a result of the investigation carried out by the Authority, it is determined that besides the automobile renting company is the data controller for the data entered into the software, since the data entered into the software is first transferred to the software and then shared with other companies, the data controllers are also the software companies. In the concrete case, automobile renting companies and software companies shall act as joint Data Controllers, since the personal data processed in this direction is unlawful, these data should be destroyed within the framework of the article 7 of the KVKK and the Regulation on the Deletion, Destruction or Anonymization of Personal Data

You can find the detail of the Decision [here](#).

05

Summary of the Decision Numbered 2022/6 Regarding the “Unlawful Sharing of Personal Data On the Internet Address Where the Registry Informations of the Company of Which the Data Subject is a Former Partner

In the complaint petition submitted to the Authority, it is stated that the name and surname are written under the title of “former partners” on the website “...”, where the registration information of the company of which the data subject is a former partner, that he/she does not have any legal or administrative ties with the company, thus he/she did not want his/her personal data to be shared with third parties without his/her consent, in this context, (s)he applied to chamber of commerce who is the data controller both in written and oral, that it was stated by the chamber of commerce that the request of the data subject could not be fulfilled in accordance with the Turkish Commercial Code and the Trade Registry Regulation. As a result of the investigation carried out by the Authority, it is determined that The personal data processing activity carried out by the Chamber of Commerce by providing the opportunity to make inquiries by entering company information from the information bank section of the website and to facilitate access to information by placing the information in the trade registry newspaper on this platform, considering that it can be evaluated within the scope of the obligations foreseen for the chambers of commerce in the Constitution and the Law on the Union of Chambers and Commodity Exchanges of Turkey Numbered 5174 and the Chambers and Commodity Exchanges, it has been determined that the personal data processing activity in question is carried out on the basis of the conditions that are clearly stipulated in the laws and that the data controller is obligatory in order to fulfill its legal obligations. Based on these evaluations, the Authority has decided not to impose any action to be taken against the Data Controller within the scope of the law.

You can find the detail of the Decision [here](#).

06

Summary of the Decision Numbered 2022/31 Regarding the “Processing of the Personal Data of the Data Subject by Data Controller Operating In the Health Sector for the Purpose of Sending Commercial Electronic Messages Without the Explicit Consent of the Data Subject”

In the complaint petition submitted to the Authority, it is stated that commercial message was sent to the e-mail address of the data subject without permission by the data controller operating in the health sector, and at the same time, there was no explicit consent for the processing of personal data by the data controller and the special conditions listed in the law code were not fulfilled. As a result of the investigation carried out by the Authority, it is determined that providing the contact information of the data subject or his/her patient companions during the opening of the patient record, does not constitute a violation of KVKK and other legislation, however, in the concrete case, the contact information of the data subject is not used for transmitting any medical information to him/her or his/her relatives, but for a marketing activity, the content of the e-mail sent to the data subject is for informational and commercial purposes, and in the aforementioned case, it has been found to have been unlawful act due to the processing of personal data by means of sending commercial e-mails to the e-mail address in an unconnected manner for the purpose of obtaining them at the time they are provided. Based on these evaluations, the Authority has decided to impose an 100.000,00 TRY administrative fine on the data controller.

You can find the detail of the Decision [here](#).

07

Summary of the Decision Numbered 2022/103 Regarding the “Sharing the Content of the File About the Execution Proceedings Started About a Company in which the Name of the Data Subject is Mentioned on Social Media.”

In the complaint petition submitted to the Authority, it is stated that after the shopping with textile company, enforcement proceedings were initiated by the data controller against the spare part company in which the name of the data subject is mentioned, and in this process, personal rights were violated by a person by means of sharing the personal data included in the execution file with third parties in a group open to everyone on Facebook, although the data subject has no commercial relationship.

As a result of the investigation carried out by the Authority, it is determined that the personal data will not be processed in sharing these documents via the social media platform by photographing the request document of enforcement proceedings by the employee of the data controller and in sharing comments including some information about the company on social media platform, and although the name and surname of the data subject is mentioned in the name of the company that is the subject of the complaint, since it is understood that the legal entity is targeted in the social media posts, the data in question will be considered as the data of a legal entity, but not a natural person.

Based on these evaluations, the Authority has decided not to impose any action to be taken against the Data Controller within the scope of the law.

You can find the detail of the Decision [here](#).

08

Summary of the Decision Numbered 2022/172 Regarding the “Requesting Sensitive Personal Data from the Candidates in the Recruitment Process by the Liaison Office in Türkiye of the Data Controller Residing Abroad.”

In the complaint petition submitted to the Authority, it is stated that when the data subject is accepted to the job, the data subject's forensic record, health report, lung film report, blood group document, photocopy of driver's license, photocopy of marriage certificate and family members' identity card photocopies were requested by the liaison office of the data controller without explicit consent, the personal data of the data subject may also transferred abroad since the data controller resides abroad.

As a result of the investigation carried out by the Authority, it is determined that the title of “Data Controller” can be attributed of the data controller residing abroad, but to the data controller himself who is a resident and legal entity abroad, the notification made by the data subject to the liaison office is deemed valid legally, , the explicit consent obtained from the data subject lawfully.

Based on these evaluations, the Authority has decided that the data controller should show maximum attention and care regarding the applications of the data subjects, it is required that the document showing that the personal data of the data subject has been destroyed at the company headquarters and liaison office should be forwarded to the data subject, and should inform the Authority about the outcome of the transaction together with the document proving this matter.

You can find the detail of the Decision [here](#).

09

Summary of the Decision Numbered 2022/184 Regarding the “Sharing the Debt Information of the Data Subject with Third Parties by a Receivables Management Corporation.”

In the complaint petition submitted to the Authority, it is stated that an SMS has been sent to the lines registered in the name of the data subject's brother and spouse who is a military personnel, under a title bearing the title of the data controller receivable management corporation, afterwards a call from a person who says that the line belonging to the spouse of the data subject is a law firm employee has been done, the personal data is shared with third parties without the consent of the data subject.

As a result of the investigation carried out by the Authority, it is determined that considering that the processing condition listed in the KVKK is not valid for recording the phone numbers calling the data controller as the phone number of the data subject and sharing the debt information with third parties by calling these phones, the data controller has not taken the necessary technical and administrative measures to ensure the appropriate level of security in order to prevent the unlawful processing of personal data.

Based on these evaluations, the Authority has decided to impose an 50.000,00 TRY administrative fine on the data controller.

You can find the detail of the Decision [here](#).

10

Summary of the Decision Numbered 2022/224 Regarding the “Sharing the Phone Number of the Data Subject with Third Parties by A Call Center of a Bank.”

In the complaint petition submitted to the Authority, it is stated that a card of the third party has been found at the bank's ATM by the data subject, and then contacted with the call center of bank who is the data controller, during the call, it has been suggested by the call center officer to receive the card from the data subject by means of sharing the phone number of the data subject with the third person who has the card, the data subject has not consented to this solution proposal, and upon request of the call center officer to deliver the card to the security guards at the airport, the data subject has handed over the bank card to the officials, however, in the following hours, a message was sent by the cardholder to the data subject via his/her personal phone number, the processed data has been transmitted to the cardholder without the explicit consent of the data subject.

As a result of the investigation carried out by the Authority, it is determined that when contacting the bank through the call center, the KVKK clarification text has been presented to the caller, also when the data subject made an application from the 'contact us' section on the website of the data controller, the box "I have read and understood the Information provided under KVKK has been checked from documents transmitted by the data controller.

Based on these evaluations, the Authority has decided not to impose any action to be taken against the data controller within the scope of the law.

You can find the detail of the Decision [here](#).

11

Summary of the Decision Numbered 2022/243 Regarding the “Processing the Personal Data By Sending the Invoice to the Data Subject, Upon Using the E-Mail Address of the Data Subject While Ordering on the Internet By a Person Who Has the Same Name.”

In the complaint petition submitted to the Authority, it is stated that a person whose name is the same with the Data Subject is a member of the Data Controller serving over the internet and placed an order, when this person was placing the order, he/she used the e-mail address of the Data Subject, without checking and confirming the accuracy of the e-mail address by the Data Controller, the invoice for the order has been sent to the Data Subject by performing the membership process. As a result of the investigation carried out by the Authority, it is determined that the data controller causes the e-mail address of the data subject who is not a party to the remote sales contract to be processed without establishing a confirmation mechanism for the recipient groups to which the invoice will be sent and the information of the sender and the receiver in the invoice to be disclosed to the Data Subject indirectly and therefore processing activity in question is in violation of the Law, various provisions of the European General Data Protection Regulation (GDPR) and evaluations were included in the defense of the data controller, and compliance with local legislation was a priority.

Based on these evaluations, the Authority has decided to impose an 100.000,00 TRY administrative fine on the data controller.

You can find the detail of the Decision [here](#).

12

Summary of the Decision Numbered 2022/662 Regarding the “Processing of the Data Subject’s ‘Hand Geometry’ Information Without Obtaining Explicit Consent by the Data Controller in Order to Enter the Service Building of an Enterprise.”

In the complaint petition submitted to the Authority, it is stated that in order for the data subject to enter the service area while registering for a business, the palm and fingerprint information have been scanned by the relevant company authorities and this data has been processed in the company records, accessing to service area is provided by placing the hands of the recipients on the device and by typing the given password, therefore, the palm and fingerprint of the data subject are scanned without a legally valid explicit consent, after the termination of the employment contract, the data controller was applied by the data subject due to an adequate answer has not been given by the data controller.

As a result of the investigation carried out by the Authority, it is determined that there is no reason for compliance with the law regarding the processing of sensitive personal data and the use of biometric data-based systems in this context, in order to control the entrances to the service building within the body of the data controller, in this context, the sensitive personal data of the Data Subject has been processed without any processing conditions in the KVKK.

Based on these evaluations, the Authority has decided to impose an 100.000,00 TRY administrative fine on the data controller.

You can find the detail of the Decision [here](#).

13

The Polish Data Protection Authority Has Decided to Impose an Administrative Fine on Warsaw Centre for Intoxicated Persons

As a result of the investigation carried out by the Polish DPA based on the data breach notifications it has been determined that data controller has been controlling and monitoring alcohol-addicted people who come for treatment, and during these surveillances, the videos and audios of the patients are recorded and stored for a long time.

The Polish DPA has been declared that the data controller violates the European Data Protection Regulation ("GDPR") due to recording voices of patients is an excessive data processing activity, since people under the influence of alcohol cannot make conscious statements and control their voices and data processing activity has no legal basis by Polish DPA.

Based on these evaluations, the Authority has decided to impose an administrative fine of 2,200 EUR on the data controller.

You can find the detail of the Decision [here](#).

14

The Polish Data Protection Authority Has Decided to Impose an Administrative Fine on Esselmann Technika Pojazdowa Sp. z o.o. Sp. k.

As a result of the investigation carried out by the Polish DPA based on the data breach notification it has been determined that data controller was found responsible for that the employee's certificate was lost including employee's personal data such as working hours, parent and childcare leave, reasons for termination the job and wages are included in the work document.

The Polish DPA has been declared that the data controller violates the European Data Protection Regulation ("GDPR") due to the data controller did not notify the Authority of the relevant violation.

Based on these evaluations, the Authority has decided to impose an administrative fine of 3,500 EUR on the data controller.

You can find the detail of the Decision [here](#).



15

The Norwegian Data Protection Authority Has Decided to Impose an Administrative Fine on Municipality of Østre Toten

As a result of the investigation carried out by the Norwegian DPA based on the data breach notification it has been determined that the systems of the data controller were attacked in January 2021. As a result of the attack, the employees of the data controller could not access most documents in the IT systems, the data of the data controller was encrypted and the backups were deleted in March 2021, on the other hand, it has been determined that the data is shared over the dark web.

The Norwegian DPA has been declared that the data controller violated the European Data Protection Regulation ("GDPR") because the data controller does not perform log analysis, does not take measures to protect the backed-up data, and does not use two-factor authentication.

Based on these evaluations, the Authority has decided to impose an administrative fine of 400,000 EUR on the data controller.

You can find the detail of the Decision [here](#).

16

The French Data Protection Authority Has Decided to Impose an Administrative Fine on TotalEnergies Électricité et Gaz France

As a result of the investigation carried out by the French DPA based on the data breach notifications it has been determined that the requests for access to the data of the data subjects and objections to receiving a call for marketing purposes are not taken into account. The French DPA has been declared that the data controller violates the European Data Protection Regulation ("GDPR") due to as the right of access to the data of the data subjects under the GDPR is not fulfilled and the data subjects are not informed about the requests they have been made.

Based on these evaluations, the Authority has decided to impose an administrative fine of 1,000,000 EUR on the data controller.

You can find the detail of the Decision [here](#).



17

The Finnish Data Protection Authority Has Decided to Impose an Administrative Fine on Otavamedia

As a result of the investigation carried out by the Finnish DPA based on the data breach notifications it has been determined that Otavamedia was found responsible due to the technical problem about e-mail forwarding, which of the data subjects were not forwarded to the customer service and this situation lasted for seven months.

The Finnish DPA has been declared that the data controller violates the European Data Protection Regulation ("GDPR") due to the data controller should be more careful when testing the e-mail inbox because e-mail is the main electronic method used by the data subjects to reach the data controller.

Based on these evaluations, the Authority has decided to impose an administrative fine of 85,000 EUR on the data controller.

You can find the detail of the Decision [here](#).

18

The Italian Data Protection Authority Has Decided to Issue a Warning on TikTok

As a result of the investigation carried out by the Italian DPA based on the data breach notifications it has been determined that data controller was found responsible due to recently changed its privacy policy and will begin to serve personalized advertisements for persons under the age of 18, so that the processing of personal data is no longer based on consent, but in the legitimate interest of data controller and its partners.

The Italian DPA has been declared that the data controller violates the European Data Protection Regulation ("GDPR") due to change in the legal basis of data processing is not in line with the GDPR and Italian Data Protection Laws, in both legal bases data subjects consents is the only legal basis for 'storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user.'

Based on these evaluations, the Authority has decided to issue a warning on the data controller.

You can find the detail of the Decision [here](#).



19

The Danish Data Protection Authority Has Banned Use of Google Workspace Application within the Municipality of Elsinore

The Danish Data Protection Authority, after the risk assessment and documents prepared by the Municipality of Elsinore ("Municipality"), determined that the Google Workspace application is not in compliance with the GDPR and that Elsinore Municipality, which acts as the data controller, does not undertake the responsibilities that should be fulfilled.

The Danish DPA has been decided that to suspend the data processing activities of the Municipality due to the transfer of data to third countries without providing the necessary protection, and to ban the use of the Google Workspace application until adequate documentation and impact assessment are provided under the GDPR.

You can find the detail of the Decision [here](#).

20

The Hellenic Data Protection Authority Has Decided to Impose an Administrative Fine on Clearview AI Inc.

As a result of the investigation carried out by the Hellenic DPA based on the data breach notification it has been determined that data controller was found responsible for violating the European Data Protection Regulation ("GDPR") due to personal data and sensitive personal data are processed without a legal basis, the obligation of transparent information and notification regarding the exercise of the rights of the data subject is not fulfilled, and access to the rights of the data subject is prevented.

Based on these evaluations, the Authority has decided to impose an administrative fine of 20,000,000 EUR on the data controller.

You can find the detail of the Decision [here](#).



21

The French Data Protection Authority Has Decided to Impose an Administrative Fine on UBEEQO International

As a result of the investigation carried out by the French DPA, it has been determined that data controller was found responsible for violating the European Data Protection Regulation ("GDPR") due to the fact that the requirements of the data minimization principle are not fulfilled, there is a lack of determination and implementation of the data retention periods, and the requirements under the GDPR in informing the data subjects are not fulfilled.

Based on these evaluations, the Authority has decided to impose an administrative fine of 175,000 EUR on the data controller.

You can find the detail of the Decision [here](#).

23

Knauf İnşaat ve Yapı Elemanları San. ve Tic. A.Ş ile Knauf Insulation Izolation San. ve Tic. A.Ş Data Breach Notification

It has been determined that a ransomware attack was carried out on the German servers of Knauf Gips KG, which is the shareholder of the data controller and has the title of data processor.

The number of people affected by the breach and whether access to the area where the personal data is located could not be determined.

You can find the details of the data breach notification [here](#) (in Turkish).

22

Meklas Otomotiv San. ve Tic. A.Ş. Data Breach Notification

It has been determined that as a result of the ransomware attack on the systems of the data controller, personal data was illegally accessed by the unauthorized third parties.

It has been stated that the groups of people affected by the breach are employees, customers, users and potential customers.

You can find the details of the data breach notification [here](#) (in Turkish).

24

Türkiye Elektrik Dağıtım A.Ş. Data Breach Notification

It has been determined that the username and password of an employee within the scope of the data controller were accessed by unauthorized third parties with an unidentified method, and the captured data was leaked by sending it to another e-mail account.

It has been stated that the groups of people affected by the breach are employees and citizens.

You can find the details of the data breach notification [here](#) (in Turkish).



25

Surtaş Otomotiv ve Servis Hizmetleri Sanayi Ticaret Limited Şirketi Data Breach Notification

It has been determined that an employee within the scope of the data controller, transmitted the confirmation code to the person who introduced herself via telephone, and the control of the online systems and instant communication application of the data controller was seized.

It has been stated that the groups of people affected by the breach are employees, customers and potential customers.

You can find the details of the data breach notification [here](#) (in Turkish).

26

NeoPets Inc. Data Breach Notification

It has been determined that a part of the systems of the data controller were cyber-attacked and the source codes and database were offered for sale, in which the seized personal data was announced by sharing on a forum site.

It has been stated that the group of people affected by the breach are users, subscribers and children.

You can find the details of the data breach notification [here](#) (in Turkish).



KVKK - GDPR

NEWSLETTER

Notification!

Contents provided in 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 without credit being given to the source is strictly prohibited. Regardless of having all the precautions and importance put in the preparation of this article, CottGroup® and its 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.

Please consult your client representative if you are a customer of CottGroup® or consult a relevant party or an expert prior to taking any action in regards to the above content.

Should you have any requests for the English translation of the announcements and decisions of the Turkish DPA, please contact us.

Prepared by



Seyma Kaplan



Selin Malkoç



Onur İzli



Öykü Solmaz



Kerem Akdağ



Civan Güneş



Seda Sallı



Berkay Koçak



Address : Astoria Towers
Kempinski Residences
Şişli / İstanbul

Telephone : +90 212 244 92 22

Fax : +90 212 244 92 21



E-mail : ask@cottgroup.com

Website : www.cottgroup.com

Website : www.verisistem.com

Follow us on Social Media...

