

# KVKK - GDPR Newsletter

## JUNE 2021



# Decision Summaries News KVKK & GDPR Reviews Of the Month;

## Summary of the Decision Regarding the “Claim that the Data Controller Did Not Fulfill the Request for Access to the Data Subject’s Personal Data about Meal Card Account Activities”

**01.** In the concrete case, the data subject requests from the company providing meal card service to access their account activities. The company sends the file containing the account activities to the data subject’s Gmail address in an encrypted form. The data subject concerns that the file in question could be accessed through identity authentication as an obstacle to accessing personal data and has requested an investigation from the Authority. As a result of the investigation, the Authority has decided that the application is reasonable implementation to fulfill the obligation to take all the necessary technical and administrative measures to ensure the appropriate level of security to prevent unlawful access to personal data.

You can find the detailed information about the Decision [here](#).

## Summary of the Decision Regarding the “Ex Officio Investigation of a Data Breach on an e-Commerce Site (Data Controller)”

**02.** The data of the data controller company that provides services for the applicants to make sales with the marketplace model, has been accessed by the partner company due to a flaw in the system. After the data breach is discovered, a confidentiality agreement is signed between the data controller and the party that has illegal access to the mentioned data.

The Authority has decided that it is not legally possible to eliminate the data breach retrospectively. In addition, it has been decided the breach that occurred because of the “search in all notifications” authorization given by the data controller to the supplier group, and that the data controller did not take the necessary measures to prevent potential damages. For these reasons, it has been decided to impose an administrative fine of 800,000 TRY on the data controller company.

You can find the detailed information about the Decision [here](#).



## Summary of the Decision Regarding the “Ex Officio Investigation about the Data Breach occurred in the Help Desk Panel Service of the Data Controller”

**03.** During the collective authorization performed in the help desk panel through a partner company on an e-commerce site, the wrong authorization is occurred. Therefore, it has been given an access to the notifications that third-party companies opened on the help desk. The data controller claimed that an error in the SQL Script code caused the incorrect authorization that led to the breach.

The Authority has stated that the data controller should be more careful in security of the information systems since it is a software company. The Authority has decided to impose an administrative fine of 300,000 TRY on the company due to insufficient security measures, faulty authorization and the lack of effective masking and control tools for the personal data included in the systems. In addition, an administrative fine of 100,000 TRY is imposed for non-fulfillment of the notification obligation.

You can find the detailed information about Decision [here](#).

## Prof. Dr. Birol CİVELEK Data Breach Notification

**04.** As a result of the cyber-attack on the data controller's cloud system, it is determined that the personal data was illegally accessed by unauthorized third parties. It has been confirmed that the data subject group affected by the breach are patients, patients' identity information and before - after photos of the healthcare services are accessed.

You can find detailed information about the data breach notification [here](#).



## INTERGEN Genetik ve Nadir Hastalıklar Tanı Araştırma & Uygulama Merkezi Data Breach Notification

**05.** As a result of the personal data copying by an IT employee working in the data controller company, it has been confirmed that the data subject group affected by the breach are employees, users, patients, and children.

You can find detailed information about the data breach notification [here](#).

## Italian Data Protection Authority Issues a Warning to the Campania Region

**06.** The Italian DPA officially has warned the Campania Region because the system that the Region planned to implement to certify COVID-19 vaccination, recovery, or negativity is in breach of privacy laws. The certification is intended to be a precondition to access several services including tourism, hotels, weddings, transportation, and entertainment. The investigation made by the Italian DPA shows that this initiative has no appropriate legal basis. It has also been stated that measures restricting the rights and freedoms of individuals can only be accepted if they are based on appropriate national legislation.

You can find the detailed information about the Decision [here](#).



## Italian Data Protection Authority Processing Limitation on a COVID19-Related App ('Mitiga')

**07.** The Italian DPA has implemented a temporary restriction on processing of personal data by the company that manages the 'Mitiga Italia' app. The app was used for the first time on May 19 to allow spectators certified as vaccinated, recovered from or tested negative for COVID-19 to access the stadium where the Coppa Italia final football match was to be held.

The restraining order of the Italian DPA states that there is currently no valid legal basis for processing of data performed to establish the Covid-free status of individuals participating public events.

You can find the detailed information about the Decision [here](#).

## Dutch Data Protection Authority Has Decided to Impose Administrative Fine on CP&A

**08.** The Dutch DPA has decided to impose an administrative fine of 15,000 EUR on CP&A for violations committed when processing the health data of the employees on sick leave.

The Authority has stated that CP&A keeps a detailed record including sensitive data on the health status of the employees on sick leave, and that these records can be accessed online without any verification system.

Based on these examinations, the Authority states that processing of personal data containing name, type, cause, and indications of the employee's illnesses for absence notification is not necessary and not legally permitted within the scope of the legislation regarding the protection of personal data. Moreover, it is stated that these should only be accessed by the authorized personnel by using multi-factor authentication system.

You can find the detailed information about the Decision [here](#).

## Luxembourg National Commission for Data Protection Has Published 18 Decisions on the Outcome of Investigations

**09.** The CNPD has released 18 decisions to public as a result of the investigations into the thematic audit campaign on video surveillance, geolocation and the role of the data protection officer.

You can find the detailed information about the Decisions [here](#).

## Green Light from Italian Data Protection Authority Subject to Adequate Safeguards

**10.** Following changes with the Ministry of Health, the Italian DPA has issued a favorable opinion on the draft decree the release of digital green certificates and laid down adequate safeguards for the use of such certificates.

The Italian DPA is requesting that the purposes for which producing a green pass may be required should be laid down clearly by way of primary legislation. Such legislation will have to provide that a green pass may only be issued and released through the national DGC platform and verified only through the "VerificaC19" app. It is states that this app will only disclose the data subject's name without displaying any other information contained whether the individual recovered from, is vaccinated against, or tested negative for COVID-19.

You can find the detailed information about the Decision [here](#).



## Swedish Data Protection Authority Finalized Investigation of 1177-Incident

**11.** The Swedish DPA's health advice service 1177 has finalized its investigation into the case of unprotected phone records being made available on the Internet.

The cause of the incident is that a network attached storage unit had been incorrectly configured and was thereby accessible on public the internet. In addition, it has been determined that encrypted communication is not used by the unit, therefore, anyone can access calls without the need for password or security protection.

You can find the detailed information about the Decision [here](#).

## Norwegian Data Protection Authority Has Decided to Impose Administrative Fine on the Municipality of Oslo

**12.** The Norwegian DPA has decided to impose an administrative fine of 40,000 EUR on the Municipality of Oslo for making documents containing sensitive personal data public.

The breach has occurred because of a letter sent to City Council's Standing Committee on Finance was not marked as "exempt from public access" by the municipal lawyer.

You can find the detailed information about the Decision [here](#).

## Norwegian Data Protection Authority Has Decided to Impose Administrative Fine on the Norwegian Confederation of Sport

**13.** The Norwegian DPA has decided to impose an administrative fine of 125,000 EUR on the Norwegian Confederation of Sport for a GDPR violation because of that personal data about 3.2 million Norwegians is available online for 87 days as a result of an error in connection with testing of a cloud computing solution.

You can find the detailed information about the Decision [here](#).



## PagoPa Has Decided to Implement the Measures Requested to Protect Users

**14.** After the Italian DPA's intervention, the data controller (PagoPA) has developed several technical measures to protect the privacy of users of the "IO" app.

PagoPA has committed themselves to minimizing user data that are transmitted to Mixpanel; in that respect, the dataset is already modified to prevent users' tax IDs and other unnecessary information from being transferred to the U.S.A. company. PagoPA will inform users adequately and request their prior consent to any data transfers to third countries; furthermore, several functions are deactivated as they allowed tracing user location via their IP address.

The Italian DPA will monitor the implementation of the measures and reserve the right to further assess adequacy of the safeguards afforded by PagoPA for data transfers to third countries.

In the light of these new measures, the Italian DPA will assess, jointly with the Ministry of Health, how to enable use of the "IO" app also for the purposes of the digital green certificates.

You can find the detailed information about the Decision [here](#).



## Dutch Data Protection Authority Has Decided to Impose Administrative Fine on an Orthodontic Practice

**15.** The Dutch DPA has decided to impose a fine of 12,000 EUR for an orthodontic practice for directing the new patients to register on an unsecured website.

You can find the detailed information about the Decision [here](#).

## Icelandic Data Protection Authority Has Decided to Impose Administrative Fine on a Company

**16.** After a minor employee of an Icelandic company that operates ice cream parlors complained to the Icelandic DPA that the area they use to change their uniforms was under constant surveillance, the Icelandic DPA has decided to impose an administrative fine of 34,000 EUR on the company.

You can find the detailed information about the Decision [here](#).



## Italian Court of Cassation Rules That Mevaluate's Algorithm Must Be Transparent for Consent to Be Valid

**17.** On May 25, 2021, the Italian Court of Cassation has decided to suspend the artificial intelligence system that analyzes, and scores the documents uploaded voluntarily by the users regarding the decision of the Italian DPA on Mevaluate Italia s.r.l in 2016, which was originally overturned by the Court of Rome. The decision of the Court of Rome, which decided that the system was legal, was overturned because the consent given by users for the data processing algorithm of Mevaluate was lacking in terms of transparency. In the decision, it has been stated that the consent can only be valid if the data subject is informed appropriately about the purposes of the data processing, and if the data subject's consents to a specific subject and with free will. In addition, it is emphasized by the Italian Court of Cassation that the consent given for their activity cannot be considered valid if the operating logic of the algorithm is not known and understood by the data subject.

You can find the details of the decision in our article on the [link](#).

# ++ 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

-  Birgül Özkahraman     Onur İzli     Şeyma Kaplan
-  Civan Güneş     Onur Saygın
-  Ece Melis Erkoçak     Selin Malkoç



### Address

Astoria Towers  
Kempinski Residences  
Şişli / İstanbul



### Telephone & Fax

Telephone: + 90 212 244 92 22  
Fax: + 90 212 244 92 21



### Web

E-mail: ask@cottgroup.com  
Website: www.cottgroup.com  
Website: www.verisistem.com

Follow Us on Social Media...

