CottGroup®
Holistic Business Services

VeriSistem®
a CottGroup® company

KVKK & GDPR NEWSLETTER

Monthly Newsletter

AUGUST-SEPTEMBER 2024

No : 2024 / 08 - 55

Decision Summaries •
KVKK-GDPR Reviews •
Data Breach Notifications •

01 Maltepe Üniversitesi Data Breach Notification

Maltepe University has notified a data breach in which a cyber attacker gained access to a user account password in the university's systems and carried out a ransomware attack to the Board. The breach occurred on June 19, 2024. The attacker demanded a ransom from the university, but no data was exfiltrated from the university's systems. Details regarding the affected groups of individuals, the number of affected individuals, and specifics about the personal data involved have not been disclosed.

Details of the data breach notification can be found here. (In Turkish)

02 Gündoğdu Mobilya Sanayi Ticaret Ltd. Şti. Data Breach Notification

Gündoğdu Furniture Industry and Trade Ltd. has notified the Board of a data breach that occurred as a result of the encryption of company data stored on servers. The breach began on August 9, 2024, and was detected on the same day. The categories of personal data affected by the breach include identity, contact, location, personnel, legal action, and customer transaction data. The number of affected individuals has not yet been determined due to a lack of access to the system. The affected data subject groups include employees, users, and customers.

Details of the data breach notification can be found here. (In Turkish)

03

Processing of Personal Data by Research Companies Using the “Random Digit Dialing Method for Telephone Interviews”

As a result of complaints submitted to the Personal Data Protection Authority (KVKK), it has been determined that some individuals, despite not sharing their phone numbers anywhere, were contacted by research companies, and during these calls, no information was provided about how their phone numbers were obtained. Upon investigation of these complaints, it was found that research companies processed personal data using the “random digit dialing method for telephone interviews.”. It was stated that in this method, phone numbers are generated randomly and automatically; however, the compliance of these practices with the KVKK was questioned.

It was determined that the explicit consent of the data subjects was not obtained during these calls, and the obligation to inform them during the initial contact was not fulfilled. According to the KVKK, the data controller conducting the calls is obligated to provide information on who is making the call, which personal data is being processed, and the purpose of the processing.

Upon reviewing the practices of the research companies, it was observed that the data was not anonymized and that only pseudonymization was used. According to Article 28 of the KVKK, if personal data is processed for official statistics by making it anonymous, the provisions of the law do not apply. However, this process was evaluated as pseudonymization, not anonymization.

As a result, the practices of the research companies were not considered within the scope of official statistics and were found to be subject to the provisions of the KVKK. In this context, it was emphasized that data controllers must take appropriate technical and administrative measures to ensure the protection of personal data and compliance with the KVKK.

You can find the details of the here. (In Turkish)

04 A Cooperation Protocol Signed Between the Personal Data Protection Authority and the Ministry of Trade

With the rapid development of digitalization, traditional methods in marketing, sales, and advertising have been replaced by digital ads and applications. In these digital environments, a large amount of data is used in targeted advertising based on personal data and deceptive commercial design (dark patterns), which poses certain risks regarding personal data privacy.

The use of personal data in ways that influence individuals' purchasing behavior has led to an inevitable intersection between personal data protection law and consumer protection law. In this context, to raise awareness about targeted advertising and deceptive commercial design practices, to follow international regulations and practices, and to develop joint policies against existing or potential violations, a Cooperation Protocol has been signed between the Directorate General of Consumer Protection and Market Surveillance of the Ministry of Trade and the Personal Data Protection Authority.

This protocol aims to increase consumer awareness about digital advertising and applications and to strengthen consumers' control over their personal data. Thus, it aims to enable individuals to act more consciously and securely in digital environments.

You can find the details of the here. (In Turkish)

05 İncirli Sağlık ve Sosyal Tesisler A.Ş. Data Breach Notification

A data breach occurred due to external interference with the company's information system, resulting in the deletion, destruction, and elimination of backups of all data, including all applications stored in the system was reported to the Board by İncirli Sağlık ve Sosyal Tesisler A.Ş. The breach has begun on August 14, 2024, and was detected on September 4, 2024. The categories of personal data affected by the breach include identity, contact, location, personnel, legal transaction, customer transaction, physical space security, health information, sexual life, biometric data, and genetic data. Due to the deletion of all records, it was not possible to determine the exact number of individuals affected by the breach; however, it is estimated that 1,000 or more individuals were impacted. The data subject groups affected by the breach include employees and patients.

Details of the data breach notification can be found here. (In Turkish)

06 Kentaş Gıda Pazarlama ve Dağıtım Ticaret Limited Şirketi Data Breach Notification

Kentaş Gıda Pazarlama ve Dağıtım Ticaret Limited Şirketi notified a data breach that subjected to a ransomware attack on September 12, 2024, resulting in the encryption of files to the Board. It is estimated that the breach affected information related to the accounting system, including invoice details, official ledgers of the data controller, debit/credit accounts, and the addresses and identity numbers of personnel registered in the system. The categories of personal data affected by the breach include identity, contact, location, customer transaction, transaction security, financial, and marketing information. No special categories of personal data were identified. It was reported that approximately 1,000 individuals were affected by the breach. The groups affected include employees, users, customers, and potential customers.

Details of the data breach notification can be found here. (In Turkish)

07 The Spanish Data Protection Authority Has Decided to Impose an Administrative Fine on UNIQLO Europe, Ltd. for Violations of GDPR Articles 5.1(f) and 32

UNIQLO has been reported to the Spanish Data Protection Authority (AEPD) regarding a request made by a former employee for access to their payroll information from July 2022. In this incident, despite the former employee only requesting their own payroll information, a company representative mistakenly sent a PDF file containing the personal data of 446 other employees via email to the complainant. This was considered a serious error that violated the confidentiality and integrity of personal data. It was determined that the company failed to fulfill its obligation to protect the personal data of its employees, thereby violating Article 5.1(f) of the General Data Protection Regulation (GDPR), which relates to the confidentiality and integrity of personal data. Additionally, the company was found to have violated Article 32.1 of the GDPR for not implementing adequate technical and organizational measures.

As a result of this breach, the Spanish Data Protection Authority (AEPD) imposed a total fine of €450,000 on UNIQLO. However, under Spanish legislation, if the company accepted the breach and voluntarily paid the fine, the amount would be reduced to €270,000. This decision highlights the serious consequences that companies may face in the event of a personal data breach and underscores the importance of complying with data protection regulations.

You can find the detail of the Decision here.

08 The Belgian Data Protection Authority Has Decided to Impose an Administrative Fine on a Telecom Operator Due to Delayed Response to an Access Request

The Belgian Data Protection Authority has imposed a fine of €100,000 on a telecom operator for violating Article 15 of the GDPR. The complainant had requested information about the processing of their personal data, specifically seeking the identities of the employees handling their data. Although the request was reviewed by two employees, it was not forwarded to the Data Protection Officer (DPO) and was only responded to after 14 months. The authority found that the complainant's access request had been partially fulfilled, but the delay and failure to involve the DPO constituted a violation of Article 15 of the GDPR.

You can find the detail of the Decision here.

09 The Swedish Data Protection Authority Has Decided to Impose an Administrative Fine on a Bank for Transferring Customer Data to Meta

A Swedish bank has reported a data breach to the Swedish Supervisory Authority (SA) regarding an incident involving the use of Meta Pixel (formerly known as Facebook Pixel). The bank stated that it used Meta Pixel on its website and application to optimize Facebook marketing, and due to the misconfiguration of the pixel, personal data was transferred to Meta between November 15, 2019, and June 2, 2021.

The categories of personal data affected by the breach include customer account numbers, loan amounts, securities asset information, and social security numbers. The bank indicated that the personal data of up to one million customers was mistakenly transferred to Meta. Upon discovering the incident, the Meta Pixel was deactivated, and Meta confirmed that the data collected through the pixel was deleted.

The Swedish Supervisory Authority determined that the data breach occurred due to the bank accidentally enabling new functions within the Meta Pixel. The affected groups include the bank's customers and application users.

This breach resulted in a violation of the GDPR, and the bank was fined approximately €1,300,000. Following the incident, the bank updated its internal procedures to ensure the correct and secure processing of personal data.

You can find the detail of the Decision here.

10 The Dutch Data Protection Authority Has Decided to Impose an Administrative Fine on Clearview for Illegal Data Collection for Facial Recognition Purposes

The Dutch Supervisory Authority (SA) has determined that Clearview AI Inc. unlawfully processed the personal data of data subjects located in the Netherlands without a legal basis. Clearview violated GDPR Article 9(1) by processing biometric data, and Articles 12(1), 14(1), and 5(1) by failing to adequately inform data subjects. Additionally, it violated other GDPR provisions by not responding to access requests and failing to appoint a representative within the EU.
The Dutch SA imposed an administrative fine of €30,500,000 on Clearview and issued four separate orders to cease ongoing violations.

You can find the detail of the Decision here.

11 The Hellenic Data Protection Authority Has Decided to Impose an Administrative Fine Following the Leak of a Personal Data File of Foreign Nationals

The Hellenic Supervisory Authority (SA) received complaints on March 1, 2024, regarding unauthorized political emails related to the European elections. Following investigations, it was found that the Ministry of Interior had unlawfully transferred the personal data of registered foreign voters for the June 2024 elections to third parties. This data included voters' email addresses and phone numbers.

The Ministry of Interior was fined €400,000 for violations of GDPR Articles 5, 25, 30, 32, and 33, and was instructed to take measures to ensure compliance. Additionally, another data controller was fined €40,000 for violations of GDPR Articles 5, 6, and 14, and ordered to delete the unlawfully processed data.

The decision regarding the New Democracy political party and other potential controllers was postponed for further investigation.

You can find the detail of the Decision here.

12

The French Data Protection Authority Has Decided to Impose an Administrative Fine of 800,000 Euros on CEGEDIM SANTÉ

During the French Supervisory Authority (SA)'s investigations it is determined that the data processed by CEGEDIM SANTÉ was not anonymous, but rather pseudonymized personal data. This means that, under Article 66 of the French Data Protection Act, the company was required to obtain the necessary authorizations to process such data. Additionally, it was found that the company violated Article 5.1.a of the GDPR by automatically downloading health data into patient records through the "HRi" teleservice, which should have been accessed by doctors for consultation purposes only. As a result of these violations, the French SA imposed an administrative fine of €800,000 on CEGEDIM SANTÉ.

You can find the detail of the Decision here.

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

Berfin Erdoğan | Ecem Başyurt | Civan Güneş | Mustafa İvgin | Özcan Bavagir | Kerem Akdağ

Adress : Astoria Towers Kempinski Residences
Büyükdere Cad. No:127 B Blok Kat:8 34394
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...