CottGroup®
Holistic Business Services

VeriSistem®
a CottGroup® company

KVKK & GDPR NEWSLETTER

Monthly Newsletter

OCTOBER 2024

No: 2024 / 10 - 56

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

01 Atılım Üniversitesi Data Breach Notification

Atılım University has reported a data breach to the Board, stating that unauthorized access was gained by a cyber attacker or attackers to the data controller's systems. Through a service within these systems, the educational information of certain individuals was queried via the Higher Education Information System of the Council of Higher Education. The breach began on May 9, 2024, and was detected on June 5, 2024. However, the exact number of affected individuals has not yet been determined. Among the affected groups are active (currently enrolled) students.

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

02 Kilis 7 Aralık Üniversitesi Data Breach Notification

Kilis 7 Aralık University has notified the Board of a data breach involving unauthorized access resulting in a violation of data confidentiality, although the source and method of the breach have not yet been determined. The start date of the breach is unknown, but it ended on September 25, 2024. It was detected on September 24, 2024, following a notification from the National Cyber Incident Response Center (USOM). The affected groups include students, customers, and potential customers.

The data involved in the breach pertains to a total of 2,747 individuals.

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

03 Lokman Hekim Üniversitesi Data Breach Notification

Lokman Hekim University, in its notification to the Board, reported a data breach related to the hosting service obtained from Natro (https://www.natro.com). The breach occurred when cyber attackers obtained login credentials to the university's customer account on Natro.com and gained unauthorized access to the account. The breach began on October 5, 2024, and ended on October 6, 2024. The personal data affected includes names, surnames, Turkish ID numbers, addresses, phone numbers, email addresses, and encrypted (MD5) website login passwords. No special categories of personal data were involved in the breach. The number of affected individuals has been reported as 2,308, including students and employees.

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

04 Irish Data Protection Commission (DPC) Has Decided to Impose an Administrative Fine on LinkedIn Ireland

The Irish Data Protection Commission (DPC) concluded its investigation into LinkedIn Ireland Unlimited Company (LinkedIn) and identified GDPR violations in the processing of user data for behavioral analysis and targeted advertising purposes. As a result, LinkedIn was fined €310 million and was instructed to bring its data processing practices in line with GDPR requirements.

The DPC found that LinkedIn did not establish a valid legal basis under Article 6 of the GDPR for processing users' personal data. The consent obtained from data subjects was deemed insufficiently informed, not freely given, or specific enough. Additionally, LinkedIn's reliance on legitimate interest and contractual necessity for data processing was found to infringe upon the rights and freedoms of data subjects, further constituting a transparency violation due to inadequate information provided. The DPC emphasized that processing personal data without a valid legal basis represents a serious breach of data protection rights.

You can find more information here.

05 European Data Protection Board Published Guidelines on Consent Requirements for Cookies and Tracking Technologies Under the ePrivacy Directive

The European Data Protection Board (EDPB) has published Guidelines 2/2023 on the Technical Scope of Article 5(3) of the ePrivacy Directive, to clarify the technical application of Article 5(3) of the ePrivacy Directive. These guidelines analyze the implications of accessing and storing information on users' devices, with a particular focus on tracking tools. In addition to cookies, the guidelines address specific cases such as IP tracking, URL tracking, and pixel tracking, examining data protection concerns posed by these emerging tracking technologies. Emphasis is placed on the need for appropriate information and consent within tracking processes to ensure user privacy.

You can find more information here.

06 Constitutional Court Decided That Dismissal of the Plaintiff's Case Due to Lack of Access to Defendant's Personal Data Violates the Right of Access to the Court Under the Turkish Data Protection Law

The Constitutional Court ruled that the applicant's right to access the court was violated due to the lack of Turkish ID number and address information for the defendants in the case petition in a elimination of joint ownership. In this case, the court requested the applicant to provide the missing information, but the applicant argued that there was no obligation to supply the Turkish ID number and address details, noting that such information was not accessible from land registry offices due to the Personal Data Protection Law (KVKK). The decision emphasized that it would be more appropriate for courts to investigate this information, and that the burden placed on the applicant was deemed unfair.

You can find more information here. (In Turkish)

07 European Data Protection Board Published Opinion on Data Processors and Sub-Processors

The European Data Protection Board (EDPB) has published Opinion numbered 2024/22, providing a comprehensive framework for data controllers on managing relationships with processors and sub-processors in compliance with the General Data Protection Regulation (GDPR). The opinion emphasizes the necessity of transparency in selecting processors, conducting risk analyses during the appointment of sub-processors, and regularly reviewing data processing agreements, all in accordance with Article 28 of the GDPR. It offers a detailed roadmap for ensuring compliance and accountability throughout all stages of the data processing chain.

You can find more information here.

08 UK Data Protection Authority Has Decided to Impose Administrative Fines on Two Companies for Sending Spam Messages

Information Commissioner's Office (ICO) has fined two finance and debt management companies a total of £150,000 for sending over 7.5 million unauthorized spam messages. Quick Tax Claims Limited received a £120,000 fine due to inadequate consent controls and unauthorized data acquisition, while National Debt Advice Limited was fined £30,000 for sending 129,902 messages. The ICO highlighted that processing data without user consent constitutes a breach of responsibility.

You can find more information here.

09 UK Data Protection Authority Has Decided to Impose an Administrative Fine on WerepairUK Ltd

Information Commissioner's Office (ICO) has fined WerepairUK Ltd £80,000 for making marketing calls to individuals without consent, including those registered with the Telephone Preference Service (TPS). The company made 42,688 unauthorized calls, violating Article 21 of the Privacy and Electronic Communications Regulations (PECR).

You can find more information here.

10 UK Data Protection Authority Has Decided to Impose Administrative Fines on WerepairUK Ltd and Service Box Group Ltd

Information Commissioner's Office (ICO) has fined WerepairUK Ltd £80,000 and Service Box Group Ltd £40,000 for making unauthorized marketing calls to nearly 50,000 individuals. It was noted that the companies targeted elderly and vulnerable people, causing considerable disturbance. The ICO has advised individuals to register with the Telephone Preference Service (TPS) to protect themselves from unsolicited calls.

You can find more information here.

11 Former RAC Employees in the UK Penalized for Data Theft

Former RAC employees were sentenced to 6 months in prison (suspended for 18 months) and 150 hours of community service for unauthorized data access and data sales. It was found that over 29,500 data records related to traffic accidents were illegally copied and transferred to a third party. The breach was detected through RAC's security systems and reported to the ICO.

You can find more information here.

12 Developments in Turkish Data Protection Law Included in 2025 Presidential Annual Program

In line with the 2025 Presidential Annual Program, efforts are aimed at aligning Turkey's Personal Data Protection Law (KVKK No. 6698) with the EU General Data Protection Regulation (GDPR). The goal is to enhance competitiveness in exports and trade within the digitalization field by harmonizing with EU legislation. This process is expected to involve collaboration between the Ministry of Justice and relevant institutions. Additionally, analyzing the impacts of EU digital economy regulations and strengthening the e-commerce infrastructure are among the primary objectives.

You can find more information here. (In Turkish)

13 UK Data Protection Authority Has Decided to Impose an Administrative Fine on PSNI

Information Commissioner's Office (ICO) imposed a £750,000 fine on the Police Service of Northern Ireland (PSNI) for disclosing the personal information of all PSNI employees. The breach occurred when sensitive information was shared in an Excel file without adequate privacy measures, putting the safety of police officers at risk. The ICO emphasized the need for stricter controls on data security processes.

You can find more information here.

14 French Data Protection Authority Has Decided to Impose an Administrative Fine on Online Fortune-Telling Companies for GDPR Violation

The French Data Protection Authority (CNIL) has imposed fines of €250,000 and €150,000 on the online fortune-telling platforms COSMOSPACE and TELEMAQUE, respectively, for processing user data without consent. The companies were found to have violated GDPR requirements by collecting sensitive data without user consent, storing it for extended periods, and sending unauthorized marketing messages.

You can find more information here.

15 EU Cyber Resilience Act Approved

The Cyber Resilience Act has been approved by the European Union Council. This legislation enforces stricter security requirements for digital products, mandating that manufacturers address vulnerabilities and provide updates. The Act aims to strengthen digital security across the EU.

You can find more information 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

Taylan Günel

Kumsal Başyurt

Berfin Erdoğan

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...