CottGroup®
Holistic Business Services

VeriSistem®
a CottGroup® company

KVKK & GDPR NEWSLETTER

Monthly Newsletter

NOVEMBER 2024

No: 2024 / 11 - 57

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

01

Zello Inc. Data Breach Notification

Pursuant to Article 12 of the Personal Data Protection Law No. 6698, Zello Inc. has reported a data breach to the Personal Data Protection Board, stemming from a ransomware attack. The breach affected 494,746 individuals, including users, subscribers, and customers, compromising personal data such as usernames, passwords encrypted with the MD5 algorithm, email addresses, and phone numbers. The breach was identified when the threat actor contacted the data controller directly. This incident highlights the critical importance of implementing strong cybersecurity measures and complying with data protection regulations to safeguard personal data and mitigate risks associated with such attacks.

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

02

Hamburg Supervisory Authority Has Decided to Impose an Administrative Fine on a Company for GDPR Non-Compliant Data Retention Activity

An investigation revealed by the Hamburg Supervisory Authority that a company operating in the debt collection sector had retained hundreds of thousands of data records despite the expiration of legal retention periods. These data retention practices were found to be non-compliant with GDPR. While it was confirmed that the data was not shared with third parties, it was unnecessarily stored for over five years. The company acknowledged the decision and cooperated with the authority, which was cited as a factor in the penalty being set at a relatively low am ount.

You can find more information here.

03 CNIL Has Decided to Impose Administrative Fines on COSMOSPACE and TELEMAQUE

The French Data Protection Authority, CNIL, has fined COSMOSPACE and TELEMAQUE for processing sensitive data without consent, retaining data longer than necessary, and sending commercial messages without user approval. COSMOSPACE was fined €250,000, while TELEMAQUE was fined €150,000. The fines were determined based on the seriousness of the violations, the impact on 1.5 million individuals, and the sensitive nature of the processed data. This decision was made in collaboration with CNIL and other European authorities.

You can find more information here.

04 Slovenian Supervisory Authority (SA) Has Decided to Impose an Administrative Fine on Fovella D.O.O.

The Slovenian Supervisory Authority (SA) has identified that Fovella d.o.o. illegally monitored its employees' using CCTV and broadcasted the footage live on the company's website. This practice was found to be in violation of national data protection laws and GDPR. The company was fined €25,000 for the unlawful processing of employees' images and failure to inform data subjects. Additionally, a formal warning was issued.

You can find more information here.

05 Norwegian Supervisory Authority (SA) Has Decided to Impose an Administrative Fine on NAV

The Norwegian Supervisory Authority (SA) has identified deficiencies in the compliance of the Norwegian Labour and Welfare Administration (NAV) with data protection regulations. Inspections initiated in September 2023 and revealed shortcomings in access management and audit logging.
As a result of these violations, NAV was fined approximately €1.7 million for non-compliance with GDPR. Additionally, various enforcement orders were issued to ensure compliance.

You can find more information here.

06 Norwegian Supervisory Authority (SA) Has Decided to Impose an Administrative Fine on Eidskog Municipality

The Norwegian Data Protection Authority (SA) has imposed an administrative fine of €21,000 (250,000 NOK) on Eidskog Municipality for violations of the General Data Protection Regulation.
Inspections revealed that the municipality unlawfully published confidential information about a whistleblower in public records and shared it unredacted with former colleagues. These breaches led to the exposure of sensitive information, including the individual's physical and mental health as well as financial status. The authority concluded that the municipality had an insufficient understanding of its confidentiality obligations.

You can find more information here.

07 Norwegian Supervisory Authority (SA) Has Decided to Impose an Administrative Fine on the University of Agder

The Norwegian Supervisory Authority (SA) has imposed an administrative fine of approximately €12,700 on the University of Agder for failing to implement necessary security measures to protect personal data.
An investigation, initiated in February 2024 after an employee discovered that personal data was stored in accessible Microsoft Teams folders without the knowledge of the affected staff, revealed that this issue had persisted since August 2018. The breach affected approximately 16,000 individuals, leading to the exposure of sensitive information. The authority concluded that the university had violated GDPR.

You can find more information here.

08 Turkish Personal Data Protection Authority Has Published an Information Note on Chatbots

The Turkish Personal Data Protection Authority (KVKK) has published the Memorandum on AI Chatbots, emphasizing key considerations for their development and use. The memorandum highlights the importance of ensuring compliance with the principles of accountability, transparency, and data minimization under Law No. 6698. It underscores the need for adequate safeguards to protect personal data, including risk assessments, privacy-by-design approaches, and adherence to international standards. Specific attention is drawn to potential risks, such as excessive data sharing by users, exploitation of technical vulnerabilities, and inadequate measures for safeguarding children's data. Developers and organizations are urged to take proactive measures, including implementing secure data transfer methods, providing clear privacy notices, and fulfilling their obligations as data controllers or processors to prevent data breaches and uphold user privacy.

You can find more information here. (In Turkish)

09 Turkish Personal Data Protection Authority Has Published a Bulletin on Parental Sharing (Sharenting) and Children's Privacy on Social Media

The Turkish Personal Data Protection Authority (KVKK) has published a bulletin containing various recommendations and warnings aimed at raising awareness about the protection of children's personal data in the digital age. The bulletin highlights the risks associated with the processing and sharing of children's personal data on social media, particularly referring to the term "sharenting," which describes parents frequently and extensively sharing information about their children. It emphasizes that parents must act more consciously and responsibly when sharing content related to their children's private lives. It is stated that such sharing, which does not serve the best interests of the child, conflicts with personal data protection legislation. The bulletin further underscores the obligation of parents with custody to protect their children's privacy. KVKK reminds stakeholders of the critical importance of adhering to the principles of proportionality, necessity, and compliance with the law to ensure data security and safeguard children's rights.

You can find more information here. (In Turkish)

10 European Commission Has Decided to Impose an Administrative Fine on Meta for Violating EU Competition Rules

The European Commission (Commission) fined Meta €797.72 million for violating EU antitrust regulations by integrating its online classified ads service, Facebook Marketplace, with its social network, Facebook, and for imposing unfair trading conditions on other online classified ads providers. The Commission determined that Meta's practice of automatically granting Facebook users access to Marketplace provided it with an undue competitive advantage, potentially marginalizing competitors. Additionally, Meta's unilateral imposition of unfair terms allowed it to exploit advertising data from rival services for the benefit of Marketplace. The Commission has mandated that Meta cease these practices and avoid similar conduct in the future.

You can find more information here.

11 Polish Data Protection Authority Has Decided to Impose an Administrative Fine on the Marathon Sports Association

The Polish Data Protection Authority (SA) imposed an administrative fine of €210 on the Marathon Sports Association (Association) for failing to notify the supervisory authority of a personal data breach. The Association organized a competition and published the participants' list on Facebook; however, while the entries appeared to display only the name, surname, gender, club, and city information, it was later discovered that hidden information was present in the file after downloading. This allowed individuals to be identified or contacted. The incident was brought to light by a third party. Nevertheless, the SA emphasized that the Association should have assessed the risk posed by such an incident and notified the supervisory authority accordingly.

You can find more information here.

12

Polish Data Protection Authority Has Decided to Impose an Administrative Fine on Res-Gastro M. Gaweł Sp. k.

The Polish Data Protection Authority (SA) imposed an administrative fine of €54.600 on Res-Gastro M. Gaweł Sp. k., a catering company, for failing to implement appropriate technical and organizational measures to ensure data security, as required by Articles 5, 24, 25, and 32 of the GDPR.

The investigation revealed that an employee lost an unencrypted flash drive containing personal data of another employee, including name, address, citizenship, gender, date of birth, personal identification number (PESEL), passport details, contact information, photographs, and salary details. The company's risk analysis was found to be inadequate, as it failed to anticipate the risk of losing such data carriers. Additionally, the company relied on instructional videos to teach employees how to encrypt files, thereby shifting the responsibility onto them, rather than implementing robust organizational policies.

The SA emphasized that the company misjudged the risk to data and lacked effective procedures to regularly test and evaluate the security measures in place. Consequently, the SA mandated that Res-Gastro adopt appropriate organizational and technical measures to ensure secure data processing.

You can find more information here.

13 Polish Data Protection Authority Has Decided to Impose an Administrative Fine on the “Stop LGBT” Legislative Initiative Committee

The Polish Data Protection Authority (SA) imposed a €2.500 administrative fine on the “Stop LGBT” Legislative Initiative Committee (Committee) for violating Articles 24, 25, 32, 33, and 34 of the GDPR. The Committee collected signatures for a petition to ban assemblies advocating LGBT rights but failed to secure the lists, leaving them unattended in a church. This negligence exposed signatories’ personal data, including names, addresses, and PESEL numbers, to unauthorized access. The Committee’s inadequate risk assessment underestimated potential breaches, and it lacked measures to protect collected data from public view. Additionally, the Committee did not notify the supervisory authority or affected individuals about the data breach. Consequently, SA mandated the implementation of appropriate technical and organizational safeguards to ensure data security.

You can find more information here.

14 Polish Data Protection Authority Has Decided to Impose an Administrative Fine on Independent Public Health Care Centre

The Polish Data Protection Authority (SA) imposed a €9,300 administrative fine on the Independent Public Health Care Centre (Centre) for violations of Articles 5, 24, 25, 32, and 34 of the GDPR. In February 2022, a ransomware attack encrypted personal data of approximately 30,000 patients and over 1,000 employees, rendering the data inaccessible. The Centre notified the Personal Data Protection Office and the police but did not inform the affected individuals, mistakenly believing the incident was not severe since the data had not been leaked. Investigations revealed that the Centre had failed to conduct prior risk analyses and lacked adequate technical and organizational measures to safeguard personal data. Consequently, the SA mandated the implementation of appropriate security measures and required the Centre to notify affected individuals about the breach, detailing the incident, potential consequences, and providing contact information for further assistance.

You can find more information here.

15

Polish Data Protection Authority Has Decided to Impose an Administrative Fine on American Heart of Poland S.A.

The Polish Data Protection Authority (SA) imposed an administrative fine of €330.000 on American Heart of Poland S.A. for violations of Articles 5, 24, and 32 of the GDPR.

A cyberattack compromised the personal data of approximately 21,000 individuals, including patients and employees. Exposed information encompassed names, parents' names, mother's maiden name, date of birth, financial details, health records, bank account numbers, addresses, personal identification numbers (PESEL), usernames, passwords, ID card details, telephone numbers, and email addresses. The SA's investigation revealed that the company had inadequately assessed data protection risks and failed to adhere to its own security policies during the pandemic. This negligence resulted in unauthorized access to sensitive personal data. Consequently, the SA mandated the implementation of appropriate technical and organizational measures to ensure data security.

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...