Forensic Response to Personal Data Breaches in *Transavia Airlines C. V.*

Daria Bulgakova

An advocate, PhD in international law, Associate professor, Department of Law and Public Administration, Zaporizhzhia Institute of Economics and Information Technologies, Zaporizhzhia, Ukraine, ORCID: https://orcid.org/0000-0002-8640-3622, e-mail: dariabulgakova@yahoo.com

The case study investigates a significant personal data breach at Transavia Airlines C. V. occurred in the Netherlands, 2021, where a vicious third party achieved unauthorized credentials to sensitive procedures, compromising millions of credit card records and personal details of passengers, workers, suppliers, and job applicants. The infringement, detected months behind it emerged, highlighted critical weaknesses in technical safeguards, including weak passwords, bypassing multi-factor authentication, insufficient network segmentation, and incomplete logging. A forensic questioning quantified the consequence, determined attack vectors, and reported corrective actions. The Dutch Data Protection Authority set a €400,000 fine for infractions of GDPR Articles 32(1) and 32(2). The case delivers noteworthy assignments for Ukrainian forensic experts and IT auditors. Also, business shall execute timely forensic analysis, robust preventive measures, and regulatory compliance are essential to protect personal data and prevent reputational and financial harm.

Keywords: *Data breach; GDPR; forensic investigation; personal data protection; network security.*

Правове значення експертного дослідження обробки персональних даних у Transavia Airlines C. V.

Дар'я Булгакова

Досліджено випадок масштабного порушення персональних даних у Transavia Airlines C. V., що стався в Нідерландах у 2021 році, коли зловмисник отримав несанкціонований доступ до конфіденційних процедур, скомпрометувавши мільйони записів кредитних карток та персональні дані пасажирів, працівників, постачальників і кандидатів на роботу. Інцидент, виявлений лише через кілька місяців, засвідчив критичну недосконалість у технічних межах захисту, включно зі слабкими паролями, обходом багатофакторної автентифікації, недостатньою сегментацією мережі й неповним веденням нет-журналів. Судово-експертне дослідження оцінило наслідки, визначило вектори атаки та надало рекомендації щодо наступних кіберзаходів з безпеки. Нідерландський орган із захисту даних наклав штраф на компанію у розмірі €400 000 за порушення статей 32(1) і 32(2) GDPR. Цей кейс має важливе значення для українських судових експертів та IT-аудиторів, підкреслюючи необхідність своєчасного експертного аналізу, надійних превентивних заходів і дотримання регуляторних вимог для захисту персональних даних і запобігання репутаційним та фінансовим збиткам.

Ключові слова: *порушення даних, GDPR; судово-експертний висновок; захист персональних даних; безпека мережі.*

The case study concerns Transavia Airlines C. V. (hereinafter — Transavia). As an airline registered in the Netherlands, Transavia operates flights for business travelers and consumers within Europe.

On 24 October 2019, the Dutch Data Protection Authority (AP) received a notification from Transavia regarding a personal data security breach as referred to in Article 33 of the GDPR. In this notification, Transavia indicated that a malicious third party had gained unauthorized access to Transavia's systems.

Following this, the AP conducted an ex officio investigation into whether the technical measures at Transavia regarding access to personal data were adequate, as referred to in Article 5(1)(f) in conjunction with Article 32 of the GDPR. The investigation focused on access to certain user accounts at Transavia, as well as the rights and capabilities these accounts had within Transavia's systems.

AP supervisors then repeatedly requested details from Transavia, which the company provided.

By letter dated 12 May 2021, the AP sent Transavia a draft enforcement notice along with the underlying report containing the findings. Transavia provided a written response to this on 28 June 2021. It is stated:

"In October 2018, GLOBALIA was informed by the credit card companies that a large number of credit cards, approximately 4,000, had been used to commit fraud. The stolen data included personal and financial information of GLOBALIA customers who made reservations or modifications on AirEuropa.com. The data did not include travel or passport information."

Other statements:

a. "The first confirmed access to GLOBALIA's network by the attacker occurred on 12 May 2018."
b. "Following this initial access, the attacker compromised a series of GLOBALIA systems, and IRIS considers that the attacker continued accessing GLOBALIA systems and accounts at least until 11 August 2018."
c. "Although IRIS has not been able to confirm how the attacker exfiltrated information from GLOBALIA's network or exactly what was exfiltrated due to limited logging, IRIS has confirmed that the attacker collected at least 488,847 unique credit cards."
d. "From the sample of 4,939 unique credit cards already reported as fraudulent, 1,185 were found in the aforementioned collection."
e. "The attacker viewed and stored in *FILE.1* at least 2,651 unique card numbers, CVVs, expiration dates, and cardholder names."
f. "In total, the attacker compromised at least 12 systems and a minimum of 2 service accounts to support their operation."
i. "Furthermore, subsequent investigations of the accounts compromised by the attacker, such as the service account GLOBALIA\EJP, revealed that it used a password that did not meet complexity and length requirements in line with best practice."

j. "Considering that most of the sensitive data collected by the attacker was found or transferred to the server ***FILE.1, and that the server also had the only viable persistence mechanism, it is likely that the attacker used ***FILE.1 as a test server from which to exfiltrate information. Similarly, a statistical analysis of firewall logs revealed that the highest number of connections to the IP address controlled by the attacker, ***IP.1, from GLOBALIA systems, occurred between 14 May and 4 June, peaking from 19 to 21 May, indicating that the attacker was actively operating. Given the volume of activity, exfiltration may also have occurred during these time frames, although the fact that the attacker accessed specific credit card–related files later in June could indicate that exfiltration also took place later in the same month."

k. "No further malicious activity attributed to the same attacker or threat actor was observed after 11 August 2018."

l. "The IP address controlled by the attacker was blocked on 15 November."

Also, AIR EUROPA states that it received only 20 communications from customers, mostly related to inconveniences caused by their bank canceling cards, without reporting any financial loss, and requesting further information. Only 3 of these communications indicated some economic damage resulting from third parties using personal data obtained in the attack. AIR EUROPA responded to all information requests from the affected individuals.

AIR EUROPA provided a risk analysis regarding the security measures for processing online sales data for AIR EUROPA passengers. This consists of a one-page document analyzing 9 risks, among them are:

(1) Article 34.3 GDPR provides three exceptions to notifying data subjects:
   - ✓ - 34.3(a). Sensitive data (special categories, addresses, phone numbers, passport/ID numbers, birthdates) was not accessed or stored with card information, making it difficult to identify individuals.
   - ✓ - 34.3(b). Banks and card issuers blocked compromised cards and informed affected customers, rendering the data useless.
   - ✓ - 34.3(c). It is nearly impossible to uniquely identify individuals from the dataset; if notification were required, a public notice would be needed, which AIR EUROPA considered burdensome with no practical benefit.

(2) According to the AEPD methodology, the quantitative threshold for notification was not exceeded (30 vs 40), though the qualitative threshold was. Despite this, AIR EUROPA chose not to notify individuals, arguing the incident posed no high risk to their rights and freedoms.

(3) In cases of high risk, exceptions under Article 34.3(a) and (b) could apply.

On 14 November 2019, AIR EUROPA informed the Agency that it is fully owned by GLOBALIA CORPORACIÓN EMPRESARIAL, with IT and communications operations managed by GLOBALIA SISTEMAS Y COMUNICACIONES under a comprehensive outsourcing contract. A data processing agreement designates GLOBALIA SISTEMAS as the processor and AIR EUROPA as the controller. The company provided a Cybersecurity Incident Response Plan and a forensic report required by PCI Council rules, which quantified compromised credit cards and guided any potential financial compensation.

The forensic investigation, initiated in October 2018, focused on assessing the extent and impact of the breach. The forensic investigation found:

(1) Conclusive evidence of a security breach at AIR EUROPA.
(2) Over 2.7 million unique credit card numbers were extracted from database systems; the attacker used tools to access plaintext data.
(3) The intrusion likely originated from unpatched, internet-facing systems, with the attacker exploiting poorly segmented servers and maintaining connections to external hosts.
(4) Exposed data included cardholder names, addresses, and expiration dates; total cards exposed were 2,722,692, though not all were at risk.
(5) The breach went undetected for months due to a sophisticated, targeted, and persistent (APT) attack, designed to evade standard security measures and erase traces.

As a result, on 23.09.2021, the DPA decided to impose a €400,000 fine on Transavia.

The case highlights the importance of robust technical safeguards, proper logging, MFA implementation, and network segmentation to prevent breaches.

Ukrainian forensic experts and IT auditors can learn from this case that in incidents involving large-scale personal data breaches, timely forensic analysis is crucial to identify root causes, assess impact, and support regulatory compliance. Implementing standard safeguards (strong passwords, MFA, network segmentation, and comprehensive logging) is critical, especially for organizations processing sensitive or high-volume personal data. Failure to apply these measures can result not only in damage to individuals' rights but also in administrative penalties and reputational harm for companies.

References

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (date accessed: 15.09.2025).
2. Transavia Airlines C. V. and Autoriteit Persoonsgegevens (2021), decision of 23.09.2021. URL: https://autoriteitpersoonsgegevens.nl/uploads/imported/boete_transavia.pdf (date accessed: 15.09.2025).