LEXING NETWORK

BALLAS PELECANOS & ASSOCIATES L.P.C.

Data Protection Authority's Fines

A short introduction to the fines imposed by the Hellenic Data Protection Authority

March 29, 2023

Nikolaos A. Papadopoulos

How does the Greek DPA handle cases of data infringements?

Plan

- Introduction
- Decision HDPA 35/2022 – Clearview AI
- Fines imposed on telecom organizations
- Data breaches
- Conclusion

Introduction

- According to the **HDPA Annual Report**, in 2021:
  - 1.160 cases were submitted before the DPA (19% rise, compared to 2020)
  - 811 cases were finalized by the DPA (16% rise, compared to 2020)
  - A total amount of EUR 414.000 of fines were imposed (almost 5 times the total amount of fines for 2020)
  - Fines were imposed on 34 cases, ranging between EUR 1.000 and 75.000
  - 181 cases of data breaches were reported (39% rise, compared to 2020)
  - 44 cases of data breaches by electronic communications service providers were reported
- Waiting for the Annual Report for **2022**…

HDPA 35/2022 – Clearview AI

- The controller sells personal identification services, including facial recognition software to law enforcement agencies in the US. The company claims to have "the largest known database of more than 10 billion facial images". It aims to reach 100 billion within the next year to make almost every person identifiable worldwide.
- Homo Digitalis, a non-profit dedicated to digital human rights in Greece, submitted a complaint with the DPA on behalf of the data subject.
- Complaints have been filed with data protection authorities in France, Austria, Italy, Greece and the United Kingdom.

HDPA 35/2022 – Clearview AI

- The DPA further found that the data processing had no legal basis and that there was a lack of transparency concerning the processing operations.
- The DPA held that the controller violated the principles of lawfulness and transparency as well as its obligations under GDPR.
- The DPA fined the controller **EUR 20,000,000** for these violations.
- The DPA further ordered the controller to satisfy the data subject's access request and stop collecting and processing subjects' data in Greek territory, using methods involved in the facial recognition service and to delete such existing data. Lastly, the DPA ordered the controller to appoint a representative in the EU.

Fines imposed on telecom organisations

HDPA 4/2022 – OTE group

- In 2020, the mobile telecommunications company COSMOTE (part of the OTE group of companies) reported a personal data breach to the HDPA caused by an external cyber attack.
- The breach included a 30 GB file of personal data for the period of five (5) days back in 2020.
- The file contained subscriber data of millions of subjects.
- The general company policy of COSMOTE regarding this kind of data was the following:
  - First, COSMOTE collected the information above.
  - Second, COSMOTE stored the data for three months and used it for its failure management system.
  - Third, after three months, they supplemented the data with their subscription plan, age, gender and average revenue per person. They "anonymized" this file, stored it for up to 12 months and used it for statistical purposes to optimise the design of its mobile network.

Fines imposed on telecom organisations

HDPA 4/2022 – OTE group

- The HDPA concluded that storing a limited subset of traffic data and not all traffic data would have sufficed for failure management. Furthermore, it held that storing the data for three months was also unnecessary for this purpose.
- COSMOTE did not properly document its Data Protection Impact Assessment (DPIA) nor demonstrate that all the risks had been considered.
- COSMOTE breached the principle of transparency. The notification was not accurate enough about the purpose of failure management. The notification did not mention the three months storage period either.
- The mechanism provided by COSMOTE, however, only pseudonymized the data, which was insufficient since COSMOTE still had access to the personal key, which could decrypt the data.
- The HDPA also found that COSMOTE and OTE did not document how their cooperation was structured, making it impossible to prove whether they complied with the principle of integrity and confidentiality, resulting to the violation of the principle of accountability.
- The HDPA fined COSMOTE **EUR 6,000,000** and OTE **EUR 3,250,000**, in total **EUR 9,250,000**.

HDPA 38/2022 - Vodafone PANAFON S.A.

- Over the course of over two years, data subjects were affected by personal data breaches in the form of unauthorized replacements of their SIM cards (**SIM swaps**). The controller would comply with unauthorized third parties' requests to change SIM cards despite allegedly carrying out an identity check to rule out fraudulent behaviour.
- The DPA held that the controller failed to implement sufficient policies and security measures to prevent fraud in the SIM card replacement process. Even the additional measures implemented after the first incidents were ineffective in preventing further exploitation of weaknesses in the controller's policy.
- The DPA also noted that in case of a data breach, the controller must inform the data subjects and the DPA about it without delay. The DPA found a violation of this provision because, in at least five incidents, the DPA only became aware of a data breach 2-3 months after it had occurred.
- The DPA imposed a fine of **EUR 150,000** on the controller.

Data Breaches

HDPA 39/2022 – COSMOTE

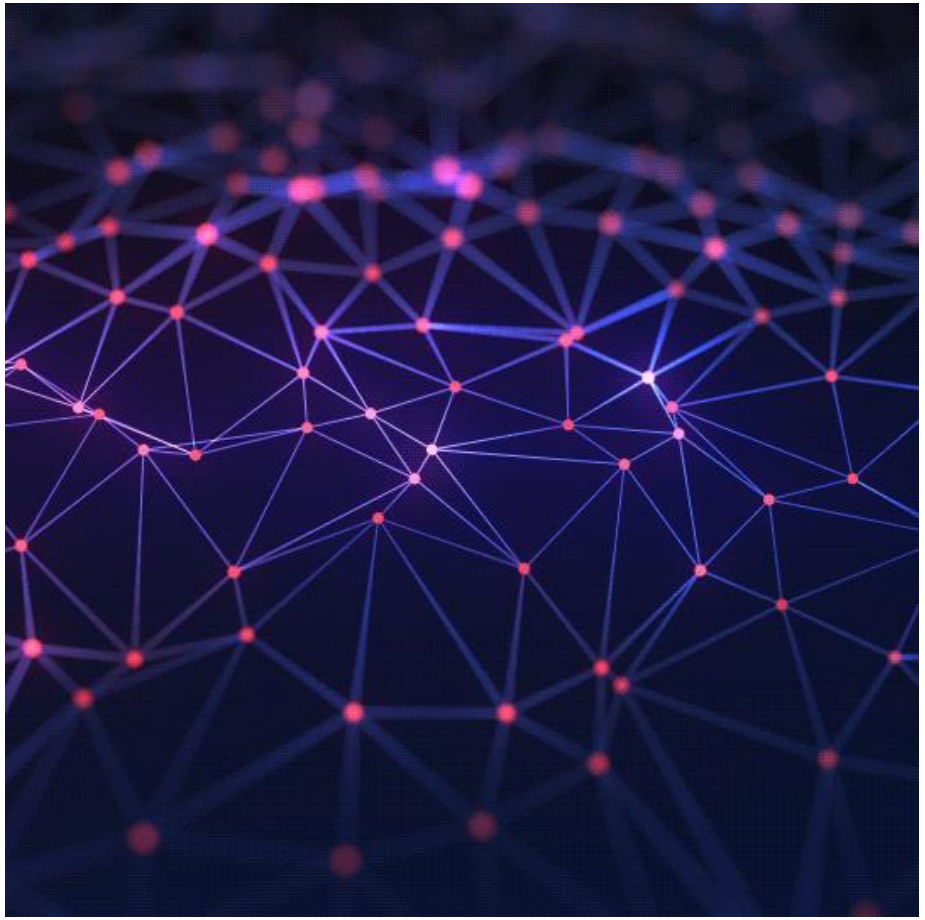
- Complaints and notifications of data breaches were submitted to the DPA related to incidents of non-compliance with the unauthorized replacement of a subscriber's sim card (**sim swap**).
- The DPA became aware of incidents of unauthorized access by malicious third parties to mobile subscriber data. The access took place following requests to change the SIM card of subscribers.
- It was attributed to problems with the identification process of subscribers when submitting such requests, either as a result of inadequate security measures or after defective implementation of existing measures.
- The DPA assessed the number of incidents, as well as the actions taken by the controller to address them and imposed a fine of **EUR 150,000**.

Data breaches

HDPA guidelines for data breaches:

- When medical test data is inadvertently sent to the wrong person, the risk for the affected subjects is high. A notification should be submitted to the DPA, and the data subject should be informed.
- In cases where medical examinations are sent by email, it is suggested that encrypted files are sent, which can only be accessed by a recipient who holds the appropriate code ("key").
- In cases of data breaches concerning credit card data, data controllers are obliged to inform any affected subjects, regardless of whether they may already be otherwise informed.
- Controllers should not waste time collecting all digital evidence before reporting data breaches to the DPA. The DPA considers the overall stance and behaviour of the data controller
- As a minimum, installing all security updates (patches) in the software applications supporting the processing should be carried out systematically and without delay.

Conclusion



Thank you!

- Q&A Session!

BALLAS PELECANOS & ASSOCIATES L.P.C.