CASE VASTAAMO

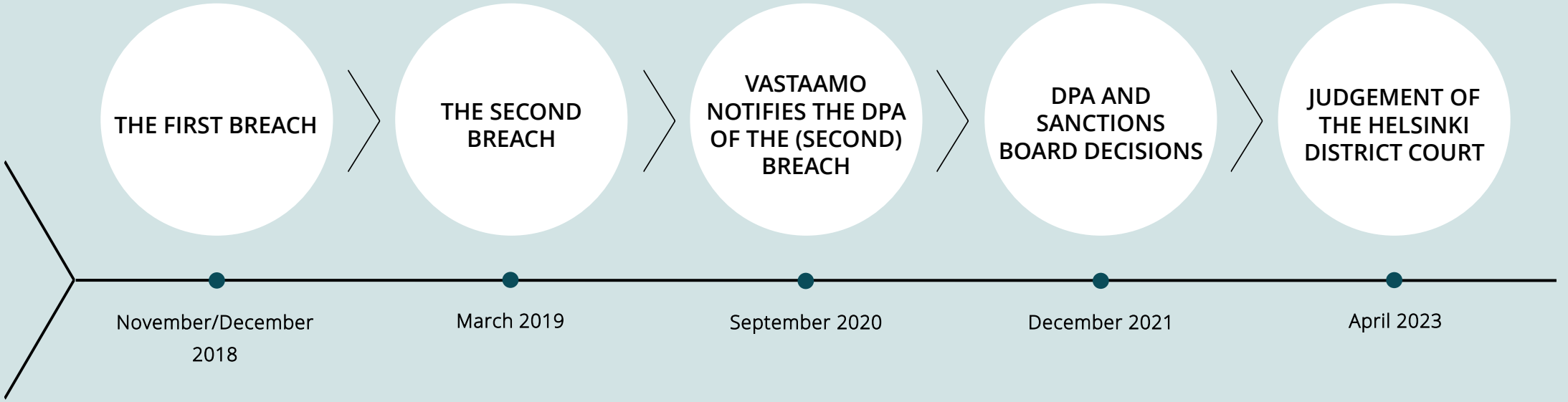
Asta Salo

25.5.2023

BACKGROUND

- The patient database of the psychotherapy centre Vastaamo was accessed at least twice by an external hacker, in November/December 2018 and March 2019.
- These breaches resulted in unauthorised access to and the loss of personal data of patients
- The patient database was likely destroyed and recovered in a single day in March 2019, when a ransom note was left on the patient information system server stating that the database had been downloaded by an attacker
    - However, the timing of the first breach in November/December 2018 and the likely risk it posed to data subjects remained unclear

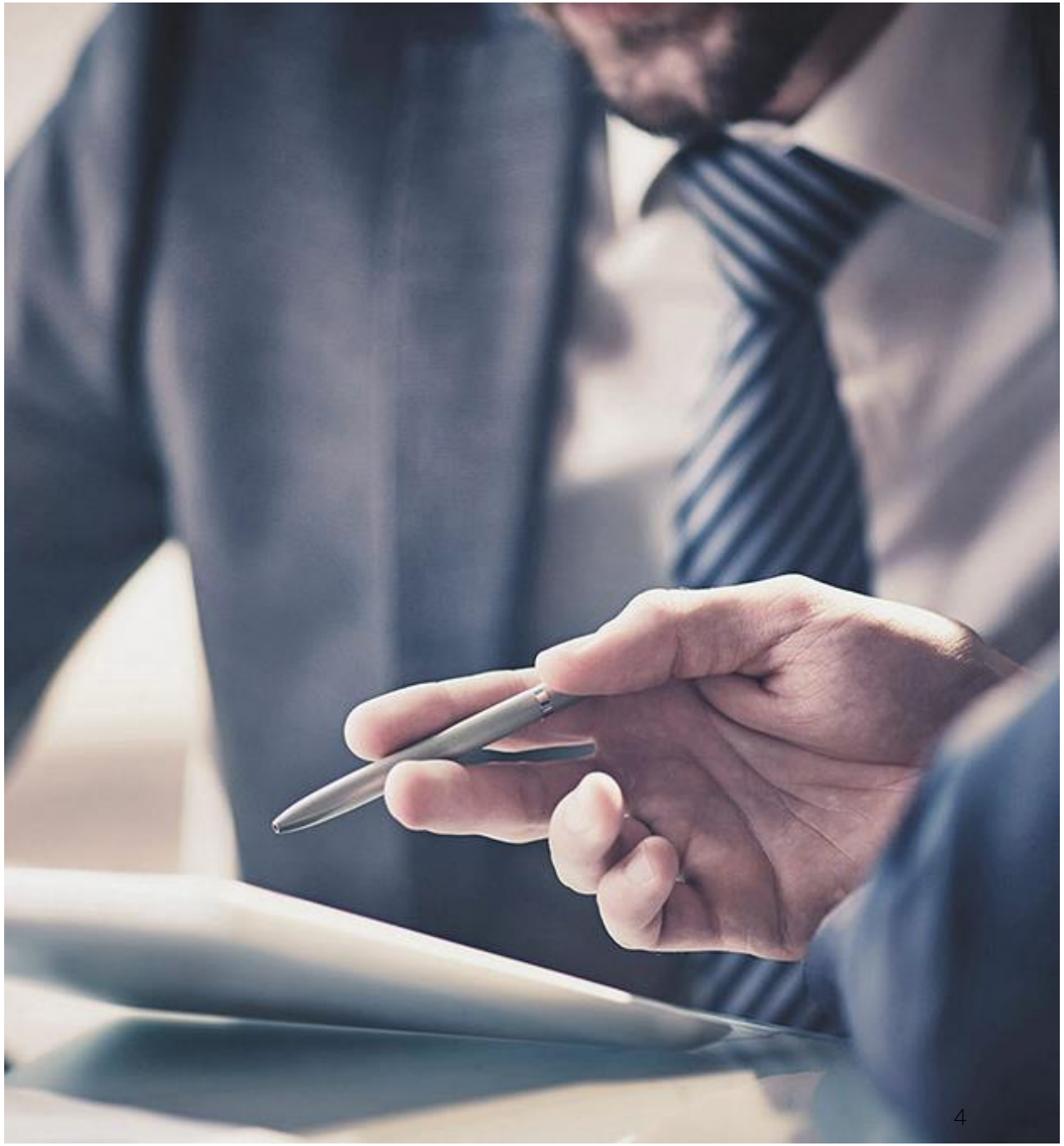
TIMELINE OF THE MAIN EVENTS



THE THREE BRANCHES OF THE CASE

1) **Administrative liability of Vastaamo**: decisions of the Deputy Data Protection Ombudsman and the Sanctions Board 7.12.2021
2) **Criminal liability of the management of Vastaamo**: Judgement of the Helsinki District Court 18.4.2023
3) **Criminal liability of the hacker**: preliminary investigation underway, approx. 24 000 victims have made a report on an offence; the case will be transferred to prosecution possibly by the end of May

+ civil compensation for victims of the data breach from the bankruptcy estate of Vastaamo



DECISIONS OF THE DEPUTY DATA PROTECTION OMBUDSMAN AND SANCTIONS BOARD 7.12.2021

PRIMARY ISSUES IN THE DPA INVESTIGATION

1) Was there a reportable incident?
2) Was Vastaamo's DPIA compliant?
3) Was there a violation of integrity and confidentiality (and related more detailed rules, e.g., Article 32)? Could Vastaamo show that it was compliant?

1. WAS THERE A REPORTABLE INCIDENT?

- Vastaamo's patient database was accessed twice by an external party. These breaches resulted in unauthorised access to personal data and the loss of personal data.
- A breach is a breach regardless of whether the data was lost accidentally or unlawfully.
- The GDPR required the controller to notify a personal data breach to
  - the supervisory authority without undue delay and, if possible, within 72 hours of its occurrence
  - data subjects "without undue delay"
- Because Vastaamo restored data from its backups, it could be found to have been aware of the loss of patient data and therefore of the security breach.
- Controller must document all personal data breaches, including the circumstances of the breach, its effects and the remedial measures taken.
  - Vastaamo had not documented the first breach in accordance with the GDPR
  - Vastaamo did not appear to have any such documented notification procedure

2. WAS VASTAAMO'S DPIA COMPLIANT?

- Vastaamo's DPIA:
  - did not sufficiently take into account the nature, scope and context of the processing, provide an adequate description of the processing activities, identify the resources used for the processing of personal data, or indicate whether records of personal data, recipients and retention periods are kept.
  - did not adequately address measures to ensure proportionality and necessity of processing and measures to protect the rights of data subjects.
  - did not adequately assess the nature, specificity, origin or threats of risks that could lead to unlawful access, unauthorised alteration or loss of personal data, nor did it adequately identify the potential impact of such risks on the rights and freedoms of data subjects.
  - did not adequately address the possibility of hacking as a potential source of risk or a threat that could lead to unlawful access, unauthorised modification or loss of personal data.
  - only considered unauthorized processing in terms of processing by a healthcare professional, not in terms of processing by an external hacker.
- As a result, Vastaamo's DPIA did not meet the requirements of Article 35(7) GDPR.

3. WAS THERE A VIOLATION OF INTEGRITY AND CONFIDENTIALITY?

- A technical investigation carried out by an outside security company found that the server for Vastaamo's patient database had not been maintained in accordance with the industry's best practice and security procedures.
- The port of the server of the medical database was not protected by a firewall and the database could have been accessed from any IP address with a default password.
  - could not have been considered protected against unauthorised or unlawful processing and against accidental loss, destruction or damage by appropriate technical or organisational measures
- The technical and organisational measures taken by Vastaamo could not be considered appropriate within the meaning of Articles 5(1)(f), 24(1), 25(1) and 32(1) of the GDPR to reduce the risks resulting from the processing of patient data to the level required for an adequate level of security of personal data.

WHO IS TO BLAME?

- As the controller, Vastaamo was responsible for any deficiencies in the security of the patient database it maintains, regardless of the cause why the database had been inadequately protected.
- When assessing the appropriate security of personal data under the GDPR, it was irrelevant who or in what capacity the persons working at Vastaamo were aware of the inadequate protection of the medical database, or whether any person working at Vastaamo was in fact aware of it.

PRIMARY ISSUES IN THE DPA INVESTIGATION

1) Was there a reportable incident? – Yes
2) Was Vastaamo's DPIA compliant? – No
3) Was there a violation of integrity and confidentiality (and related more detailed rules, e.g., Article 32)? Could Vastaamo show that it was compliant? – Yes (No)

SANCTIONS

- The Deputy Data Protection Ombudsman issued a reprimand and the Sanctions Board imposed an administrative fine of 608,000 euros (approx. 4.1 % of turnover) on Vastaamo for
  - failure to comply with obligations relating to secure data processing;
  - failure to comply with obligations relating to the notification of a security breach; and
  - failure to demonstrate compliance with data protection legislation via drafted documentation.
- The decisions are not final and may still be appealed.

JUDGEMENT OF THE HELSINKI DISTRICT COURT 18.4.2023

A BRIEF SUMMARY

- Three months of suspended imprisonment for Ville Tapio, managing director of Vastaamo for **data protection offence**
  - "Tapio -- has failed to implement pseudonymisation and encryption of personal data processed at Vastaamo as required by the GDPR.“
- The prosecutor decided not to prosecute two employees of the IT department of Vastaamo, whose actions were investigated in the preliminary investigation.
- The judgment may still be appealed and is not final.

PROSECUTOR'S MAIN CHARGES (I)

Tapio, intentionally or at least through gross negligence, as the person ultimately responsible for the security of the data, data protection and personal data processing of Vastaamo by virtue of his position and the performance of his duties,

1) failed to **document and report the data breach** of 15 March 2019 to the Finnish DPA and the National Supervisory Authority for Welfare and Health *(this charge was dismissed);*

2) breached the GDPR (Art. 32) by failing to fulfil his responsibility to **ensure the integrity and confidentiality of personal data** in Vastaamo's operations (organisational and technical implementation);

3) failed to implement the necessary technical measures referred to in the GDPR, such as **pseudonymisation and encryption of personal data**, and failed to ensure the confidentiality and integrity of the operating systems; and

PROSECUTOR'S MAIN CHARGES (II)

4) failed to implement the procedure described in Article 32(1)(d) of the GDPR to regularly **test, examine and evaluate** the effectiveness of technical and organisational measures to ensure the security of data processing (*this charge was dismissed*).

- The measures taken following the data breach of 15 March 2019 have been inadequate and therefore the security of the patient database, which contained sensitive personal data on the treatment of individuals, had been compromised until 21 October 2020.

SOME EXTRACTS FROM THE JUDGEMENT

- The data in the medical database of Vastaamo was readable in plain language from the server and was not encrypted within the database. The patient database had contained, *inter alia,* customer contact details and patient records.
- The contact details and the records from patient visits had been separated into separate tables, which could be linked to each other by a key on the tables. The databases had not been separated -> this was not adequate pseudonymization.
- Tapio had been aware of the data breach and tried to conceal it from the company which later acquired Vastaamo.
    - However, since Vastaamo's data security practices were blatantly inadequate both before and after the data breach, it was in fact irrelevant whether Tapio was aware of the data breach of 15 March 2019
- Failure to document and report the data breach is not criminalised under the Finnish Criminal Code (instead, Vastaamo was fined for this by the Finnish DPA)

THE JUDGEMENT

- District Court: “Tapio has committed a data protection offence by failing to implement the requirement of the GDPR for pseudonymisation and encryption of personal data processed at Vastaamo. In all other respects, the charges are dismissed.”

Thank you

Asta Salo
+358 44 553 6868
asta.salo@castren.fi

www.castren.fi