REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

[redacted]

Ours: 04.11.2021 nr 2.2.-2/20/3028

Reprimand for failure to comply with the requirements of the General Data Protection Regulation & notice of termination of the proceeding in regard to the protection of personal data

RESOLUTION:

Reprimand in a personal data protection case in which [redacted] has violated the following norms arising from the General Data Protection Regulation (GDPR): article 5 (1) f and 32 as whole.

Case

The Data Protection Inspectorate received a notice of infringement from [redacted] (AM), according to which customers and persons of [redacted] who are interested in your service but have not yet entered into a contractual relationship have reported fraudulent calls from third parties. The services and investment opportunities of various companies have been offered in fraudulent calls. Based on the procedures and tests performed by [redacted] in cooperation with an independent information security expert, you found that a leak had occurred in [redacted]'s customer management system and that the personal data of customers had been accessed.

Upon closer inspection, you identified an automated script that queries the data. Immediately after finding those computers, [redacted] disconnected them from the computer network. In addition, computers were scanned with [redacted] antivirus and operating systems were reinstalled. [redacted] also examined the found artifact, but since it was encrypted, further investigation into the nature and origin of the script was not possible. [redacted] also made a so-called copy of the infected computers (using the following software [redacted]) in order to examine the artifact later, if possible. After the removal of these computers, the number of customer inquiries to [redacted], which mentioned that they had been contacted by third parties, decreased significantly. Due to the fact that in February 2021 there were no more new cases, [redacted] decided to consider the incident over.

You confirmed that the data leak was made possible due to insufficient security measures.

We clarify that when processing personal data, the controller must ensure that personal data are processed in a way that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing, using appropriate technical or organizational measures (see Article 5 (1) (f) and Article 32). The controller must also take measures to reduce human error. It is currently clear that [redacted] had not implemented adequate safeguards to protect personal data.

In order to ensure security and to prevent processing in breach of the General Data Protection Regulation, the controller must assess the risks associated with the processing and implement measures to mitigate those risks, such as encryption. Taking into account the latest scientific and technological developments and the costs of implementing the measures, those measures should ensure the necessary level of security, including confidentiality, appropriate to the risks and the nature of the personal data to be protected. The data security risk assessment should consider the risks arising from the processing of personal data, such as the accidental or unlawful destruction, loss, alteration and unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed, which may in particular result in physical, material or non-material damage.

Taking into account the fact that[redacted]:

1) prepared a plan to train employees in the field of information security;
2) mapped the scope of the incident and identified a system that enabled the unauthorized processing of personal data by third parties;
3) informed the data subjects affected by the violation;
4) checked the logs of the databases of their systems, including the access logs of the employees, and included the help of the company Cybers, which specializes in information security, to help improve the situation.
5) initiated a project to transfer customer data to a database limited by even stricter security requirements;
6) perform regular stress tests on existing as well as new systems;
7) reviewed the restrictions on access to all databases and limited the number of users who can access sensitive customer information;
8) audited the users of the customer management software;
9) audited all user accounts that have access to the customer data database;
10) prepared instructions for customer support / sales department on how to help and what data to collect from persons who turn to [redacted] for a given violation;
11) implemented a comprehensive security solution, which is the [redacted] solution offered by [redacted], which helps to prevent the occurrence of similar incidents in the future;
12) checked the security of the mobile app;
13) performed compliance control of information security standards and requirements; and
14) has been able to stop the leakage by taking appropriate measures

we close the supervision procedure and reprimand Article 58 (2) (b) of the General Data Protection Regulation and draw attention once again to the following:

- the controller is obliged to ensure that personal data are processed in a way that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing, using appropriate technical or organizational measures;

- no one is protected from cyber attacks, but considering the circumstances presented, it was possible to prevent the data leakage, which is why it is important to emphasize that ensuring the security of information systems (incl. Their continuous monitoring and updating) must be regular. Therefore, possible bottlenecks must be prevented and, if necessary, information security specialists must be hired to audit the systems in order to ensure the protection of personal data.

Kind regards

/signed digitally/
[redacted]
lawyer
authorised by Director General