ANDMEKAITSE INSPEKTSIOON

FOR INTERNAL USE
Holder of information: Data Protection Inspectorate
Indication made: [redacted].2024
The access restriction applies until: [redacted].2029
For P 2 until entry into force of the Decision
Base: Section 35(1)(2), Section (1)(18[2]) of the PIA

All SA's

Our [redacted] 2024 No [redacted]

ARTICLE 60 FINAL ADOPTED DECISION
Reprimand and termination of the proceedings

Circumstances
[redacted] (registry code [redacted]) submitted a data breach notification to the Estonian Data Protection Inspectorate (Estonian DPI) on [redacted], according to which a personal data breach occurred in connection with the processing of personal data on [redacted] intended for the customers (companies) of [redacted].

According to the breach notification, an attack and data leak on [redacted] took place early in the morning on [redacted]. An unauthorized third party had found an [redacted] error in one [redacted] and used it to download and modify employee records. In the afternoon of [redacted], some customers (companies) informed the controller that their employees would no longer be able to access the system. By the morning of [redacted], all major customers of the controller had contacted customer support with the same access concern. The attack and data leak were detected by [redacted] in the evening of [redacted] in the server logs. The categories of personal data affected by the breach were: first and last name, personal identification number, telephone number, job information. According to the breach notification, the persons had not been informed of the breach, but it was planned to do so.

Since not all the circumstances of the infringement were exhaustively set out in the breach notification, the Estonian DPI started a supervisory procedure on the basis of Section 56(3)(8) of the Personal Data Protection Act.

Proceedings
The Estonian DPI submitted several inquiries and proposals to the controller in the context of the supervisory procedure.

The total number of persons concerned by the data breach was 4,029, [redacted]. The Estonian DPI started LSA and CSA identification procedure under Article 56 of the General Data Protection Regulation (GDPR). As [redacted] is a company operating in Estonia, the leading supervisory authority in the supervision proceedings is the Estonian DPI.

[redacted] explained to the Estonian DPI that it is the controller of the [redacted] within the meaning of Article 4(7) of the GDPR.

The controller explained that on the afternoon of [redacted], the customer support began to

receive complaints that the employees of the customers did not have access to the environments of their company. Initially, customer support was simply trying to restore access rights. On the evening of [redacted], customer support informed the development team that during the day there have been access problems with several accounts. Subsequently, the performance of the affected customers' environments was only checked at the level of the client applications (web and mobile applications). In the early morning and in the morning on [redacted], customer support received additional complaints from all major customers. All information was forwarded to the development team, but as it was a weekend and there is no 24-hour or weekend guarding in the development team, the situation started to be investigated in more detail only in the evening.

The controller explained that no comprehensive security testing or security audit had been carried out before the incident took place. However, as of [redacted] There is no [redacted]. Unfortunately, [redacted]. In addition, the controller has pointed out that [redacted].

In addition, the controller noted that the [redacted] team is extremely small in relation to the operations of the company. Due to personnel movements, there is currently only one developer in the development team who has the necessary [redacted]. Since the incident, the focus has been on correcting other similar errors to prevent potential further data leaks.

As regards the notification of data subjects, the controller explained that the incident was notified to its customers, i.e. companies that contacted customer support between [redacted] and [redacted] in connection with this incident. Other affected customers shall be communicated in accordance with the customer agreement concluded with them.

The Estonian DPI asked the controller to specify whether data subjects had been informed of the breach and, if not, to explain, inter alia, on the basis of Article 34 GDPR, why notification was not deemed necessary. The controller indicated to the Estonian DPI that the data subjects were not informed of the breach because, in the view of the controller, the breach would not result in a high risk to the rights and freedoms of the data subject. Furthermore, the controller added that the personal data affected by the incident relate only to the professional activities of the data subject and not to their private life.

The Estonian DPI did not agree with the explanations of the controller and suggested informing the data subjects and sending a confirmation. The Estonian DPI explained to the controller that certain types of data individually may not pose a high risk, but if the data are processed together, they may be used, among other things, for fraudulent purposes. When submitting a breach notification, [redacted] has itself assessed that a person may be deprived of control over their personal data, there is a risk of identity theft, fraud, reputational damage and loss of trust. The number of data subjects affected (4029) further increases the risk. It must be considered that the breach was caused, among other things, by a malicious attack, the intentions of the attacker are unknown, and the recipient of the data cannot be considered reliable. Thus, the data processor cannot assume that the attacker will not use the data that came to him or her during the attack or will delete it from himself or herself. The Working Party on Data Protection has provided guidance that, in case of doubt, the controller should be more cautious and inform data subjects of the breach.[1]

The controller sent to the Estonian DPI a template for the notification to be sent to the data subjects

[1] Guidelines of the European Data Protection Working Party on the notification of a personal data breach under Regulation 2016/679, 06.02.2018, WP250rev.01, p. 26.

and, after receiving feedback, the controller confirmed that the notification was sent to the data subjects in relation to the personal data breach.

The position of the Estonian DPI

Pursuant to Article 24(1) GDPR, the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that personal data are processed in accordance with the GDPR, taking into account the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. Article 32(1) GDPR requires the controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including ensuring the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data. Pursuant to Article 32(2) GDPR, the assessment of the necessary level of security shall take into account, in particular, the risks posed by the processing of personal data, in particular the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The same obligation arises from the principles of personal data processing, namely Article 5(1)(f) GDPR, according to which personal data must be processed in a manner that ensures appropriate security and protects against unauthorised or unlawful processing using appropriate technical and organisational measures.

Article 4(1) GDPR defines personal data as any information relating to an identified or identifiable natural person ('data subject'). The [redacted], against which the attack took place, contained the data of employees of customers, i.e. legal persons, such as name, personal identification code, telephone number, information about the workplace, which is personal data. The collection, storage, use, etc. of such data is considered to be processing of personal data within the meaning of Article 4(2) GDPR.

According to Article 4(12) GDPR, 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Pursuant to Article 31 GDPR, the controller shall cooperate with the supervisory authority at its request in the performance of its tasks.

In order to ensure security and to prevent processing in breach of the GDPR, the controller should assess the risks involved in the processing and implement measures to mitigate those risks, such as encryption. Taking into account the state of the art and the cost of their implementation, those measures should ensure an appropriate level of security, including confidentiality, commensurate with the risks and the nature of the personal data to be protected. When assessing the data security risk, consideration should be given to the risks posed by the processing of personal data, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, which may, in particular, result in physical, material or non-material damage.[2]

[redacted] had not implemented adequate safeguards for the protection of personal data on its platform, as an unauthorised person had the opportunity to access the system and personal data. There were no adequate and functioning processes [redacted]. The attack was detected due to repeated complaints from customers (i.e. thanks to an external source). The attack occurred due to a [redacted], with the controller noting that the previously [redacted]. In addition, no comprehensive security testing or security audit has been carried out. As an explanation, the controller has pointed out that the team is small and there is currently only one developer in the development team who has the

[2] Recital 83 of the GDPR

necessary [redacted].

Nobody is protected from cyberattacks, but in order to prevent this, the controller must ensure the security of information systems and the systems must be regularly monitored to identify any risks that may have arisen. In the case of this incident, a data leak would have been avoidable if modern security measures had already been implemented earlier, which would have prevented the leakage of personal data in a cyberattack. The data controller must also ensure the effectiveness of organisational measures to ensure regular monitoring of the data processing processes in order to detect any problems encountered as soon as possible. The attack took place over the weekend and was delayed due to the small size of the team.

In this case, [redacted] either did not assess the risks of attacking [redacted] or assessed the risks as too low and thus incorrectly. Therefore, the controller did not design and implement adequate technical and organisational measures that could have resisted the attack.

Pursuant to Article 34(1) GDPR, the controller shall communicate a personal data breach to the data subject without undue delay where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. If the controller has not yet communicated the personal data breach to the data subject, the supervisory authority may, after assessing whether the personal data breach is likely to result in a high risk, request it from the controller (Article 34(4) GDPR). In this case, the DPI made a proposal to the controller to notify the data subjects of the breach.

The provision of information to individuals enables the controller to communicate, as a result of the breach, the risks and steps that data subjects affected by the breach can take to protect themselves from possible consequences. In other words, communication of a personal data breach helps protect individuals and their personal data. In addition, communication helps to prevent other potential breaches, as attacks against controllers have also occurred through their employees. Thus, by informing the data subjects, [redacted] is also able to protect its customers who are legal persons against possible attacks.

Since the controller did not understand when submitting the breach notification that in case of a high risk, data subjects must be informed, whereas the data subject is not his or her legal entity client and in addition assessed the risk as lower, we recommend that the controller trains his employees with regard to data protection. In addition, we advise the controller to create a register of personal data breaches if this has not yet been done, as any personal data breach must be documented.[3]

In addition to the above, we emphasise that any processing of data (including collection and storage) should be carried out for a specific and legitimate purpose, and personal data may be processed only if the intended purpose cannot be achieved by other means.[4] Personal data should not be collected just in case, but the processing of personal data can only take place if the purpose of the processing cannot be reasonably fulfilled by other means. The controller explained that some of the data can be entered by customers in the [redacted] platform on a voluntary basis (e.g. personal identification number, telephone, position). In addition, the data processor has indicated in the case description that the [redacted] and [redacted] data fields were removed from the employee record data model as they are not critical for the operation of the application. Therefore, we recommend that the data controller assesses whether the collection of specific data (even if the data field is filled in voluntarily) is necessary for a specific purpose. The controller (here [redacted]) is responsible for compliance with the principles set out in the GDPR and must be able to prove compliance with the principles at any time.

In conclusion, in the opinion of the Estonian Data Protection Inspectorate, [redacted] has

[3] We recommend that you get acquainted with: Estonian Data Protection Inspectorate. General instructions of the processor of personal data, 19.03.2019.
[4] Article 5(1)(a) of the GDPR lays down the principles of 'purpose limitation' and (c) of 'data minimisation'.

violated security requirements, in particular the obligations arising from Article 5(1)(f) and Articles 24 and 32 of the General Data Protection Regulation.

In addition to the above, the Inspectorate takes into account the fact that the controller cooperated with the Estonian DPI, and the controller has also confirmed that the security errors and similar security errors that caused the violation have now been corrected and the data subjects have been informed of the personal data breach.

Based on the above and on Article 58(2)(b) GDPR, the Estonian Data Protection Inspectorate issues a reprimand to [redacted] and terminates the present supervision proceedings.

In addition to the above, we make the following recommendations to [redacted]:

1. Review [redacted] to prevent similar cases.
2. Review the rights of the accounts (as [redacted] according to the case description).
3. Delete inactive accounts (including inactive test accounts).
4. Regularly train their staff to be aware of data protection requirements, including how to deal with a personal data breach.
5. Assess whether the processing of personal data complies with the principle of minimality (including whether the collected personal data is necessary for the fulfilment of the purpose).

This decision may be challenged within 30 days by submitting one of the two:

- A challenge to the Director General of the Estonian Data Protection Inspectorate pursuant to the Administrative Procedure Act[5], or
- An appeal to the administrative court under the Code of Administrative Court Procedure[6] (in this case, the challenge in the same matter can no longer be reviewed).

Yours sincerely,

[redacted]
Lawyer
Under the authority of the Director-General

[5] https://www.riigiteataja.ee/en/eli/527032019002/consolide
[6] https://www.riigiteataja.ee/en/eli/512122019007/consolide