The Norwegian Data Protection Authority expresses serious criticism of Elgiganten A/S

Date: 20-06-2022

Decision

Private companies

Serious criticism

Complaint

Treatment safety

Unauthorized access

Risk assessment and impact analysis

The Danish Data Protection Authority expresses serious criticism in a case where Elgiganten A/S had a returned television stolen during a break-in at their warehouse, which had not been reset to zero for the complainant's personal data.

Journal Number: 2021-31-5743

Summary

In June 2021, Elgiganten A/S took back the complainant's used television. While the television was being processed for reset, it was temporarily placed in the store's warehouse. The placement outside was due to a lack of space and a hectic situation inside the store, where products are normally placed in an area to which only employees have access. In the meantime, the department store was subjected to a burglary. This meant that a third party gained access to the complainant's television and thus to information from various streaming services that the complainant was logged into, as well as the complainant's browsing history.

Before the break-in, the electricity giant had carried out a risk assessment for theft of their products and assessed the risk to be high. Therefore, the warehouse was secured by locking, a high wall, surveillance cameras and motion sensors. However, the burglar gained access by punching a hole in the high wall.

The risk assessment must also include scenarios such as great work pressure

The Norwegian Data Protection Authority determined in the case that the data controller must ensure that products are stored with sufficient security and are subject to measures that match the risk of various abuse scenarios. As the Elgiganten assessed that the risk of theft of products was high, and as it is generally known that employees do not always comply with

internal procedures, risk scenarios such as high work pressure and lack of space should have been included in the risk assessment. In other words, the electricity giant should have taken into account that employees may deviate from the established procedures – e.g. in case of lack of space and high work pressure.

Decision

The Danish Data Protection Authority hereby returns to the case, where [complainant] complained to the Danish Authority on 10 November 2021 that Elgiganten A/S did not delete the content on the television when the complainant returned a purchased television, with which a third party gained access to the complainant's streaming services , including insight into data from the complainant's used services and browsing history.

1. Decision

After a review of the case, the Data Protection Authority finds that there are grounds for expressing serious criticism that Elgiganten A/S' processing of personal data has not taken place in accordance with the rules in the data protection regulation[1] article 32, subsection 1.

Below follows a closer review of the case and a rationale for the Data Protection Authority's decision.

2. Case presentation

It appears from the case that Elgiganten A/S received the complainant's television on 19 July 2021. The television was placed in the store's warehouse, after which it was stolen in a burglary. The television had not yet been reset according to current procedures, which is why the complainant's personal data was still stored on the television.

2.1. Complainant's comments

The complainant has stated that, in connection with a complaint case, he has handed in his television to the Elgiganten. The complainant subsequently discovers that an unauthorized third party is using his streaming services via the returned television, which should have been sent for destruction. The complainant has also noted that the television still contains data from free services and browsing history.

2.2. Elgiganten A/S' comments

Elgiganten A/S has stated that they received the complainant's television on 19 July 2021.

According to Elgiganten A/S, the reason for the incident is that an employee in the store – due to a lack of space inside the store and a stressful situation – has placed the television in the store's warehouse. There has been a burglary here, with which

the television was stolen.

Elgiganten A/S has stated that the farm is secured by; that it is locked, there is a high wall around it and surveillance cameras and motion sensors are installed. These measures have been implemented on the basis of Elgiganten's high risk assessment for theft of both new and used products. It appears that it is this high wall that the burglar broke through and thereby gained access to the television.

Elgiganten A/S has stated that it is normal procedure for personal data to be deleted regardless of whether a product is to be resold or destroyed. It is the operations team at the store, including the service department, that is responsible for resetting to factory settings of returned televisions. The television was being processed, which is why the deletion hadn't happened yet.

Elgiganten A/S has stated about their previous measures that it is not normal procedure for products that are being processed and must be reset to be left outside. The normal procedure is for the products to be placed in an area to which only employees have access and for personal data to be deleted before it is sent for destruction.

Elgiganten A/S has further stated that, based on the incident, they intend to install a roof on the warehouse. In addition, they will tighten the established routines towards the employees, including that goods may not be placed in the warehouse, even if it is secured and a roof has been fixed.

Finally, Elgiganten A/S has stated that they have guidelines for handling security breaches. This is reflected in the training of new employees. The employees do not assess the seriousness of a potential breach themselves, but are – after creation in the case management system – assigned to a specific employee who is responsible for handling security breaches in Elgiganten or Elkjøp Nordic. Based on the incident, Elgiganten will tighten and evaluate the routines going forward.

3. Reason for the Data Protection Authority's decision

The Danish Data Protection Authority assumes that Elgiganten A/S – at the time of the return of the television – has become the data controller for any information that may be stored on the device, cf. Article 4, No. 7 of the Data Protection Regulation.

Based on the information provided by Elgiganten A/S, the Danish Data Protection Authority assumes that there has been unauthorized access to the complainant's personal data, which is why the Danish Data Protection Authority finds that there has been a breach of personal data security, cf. Article 4, No. 12 of the Data Protection Regulation.

3.1. Article 32 of the Data Protection Regulation

It follows from the data protection regulation article 32, subsection 1, that the data controller must take appropriate technical

and organizational measures to ensure a level of security appropriate to the risks involved in the data controller's processing of personal data.

The data controller thus has a duty to identify the risks that the data controller's processing poses to the data subjects and to ensure that appropriate security measures are introduced to protect the data subjects against these risks.

The requirement in Article 32 for adequate security will normally mean that you as the data controller must ensure that information about data subjects does not come to the knowledge of unauthorized persons.

When assessing the risk, it must be included that information about a registered person's browsing history may constitute personal data of special categories. In addition, unauthorized access to the device can create access to financial information, including credit card information, if the data subject's streaming accounts and TV subscriptions are linked to the same device.

The data controller must ensure that storage takes place with sufficient security, in which the risk of various misuse scenarios must be reflected in measures adapted to this.

Devices such as computers, telephones and TVs have a particularly high risk profile for e.g. theft. The units in question typically also contain a plurality of personal data.

It is generally the Danish Data Protection Authority's opinion that personal data on portable devices or devices with a higher risk of theft must be encrypted, or data deleted in an irrevocable manner, before the devices are put into storage.

Furthermore, the Danish Data Protection Authority is of the opinion that the data controller must ensure that all employees in the company are, to the extent necessary, familiar with any internal procedures for handling personal data, including in relation to the deletion of personal data when customers return used goods, and that procedures, guidelines etc. and workflows are continuously updated.

Based on the above, the Danish Data Protection Authority finds that Elgiganten A/S - by not having ensured that returned used products with personal data were deleted or stored sufficiently securely during processing - has not taken appropriate organizational and technical measures to ensure a level of security that suits the risks involved in the company's processing of personal data, cf. the data protection regulation's article 32, subsection 1.

After a review of the case, the Danish Data Protection Authority finds that there are grounds for expressing serious criticism that Elgiganten A/S' processing of personal data has not taken place in accordance with the rules in the data protection regulation, article 32, subsection 1.

When choosing a response, the Danish Data Protection Authority emphasized that Elgigantens A/S's measures in this case were not necessary, given the inherent risk of break-ins and theft of products that may contain personal data. This was known to Elgiganten A/S and expressed in the risk assessment. The Danish Data Protection Authority is of the opinion that employees' failure to comply with internal procedures is a known error, and control measures should have been incorporated into Elgiganten A/S's business procedures, given that risk scenarios - due to high work pressure and lack of space - should have been included in the assessment .

In addition, the Danish Data Protection Authority has emphasized that insufficient deletion concretely increases the risk of the data subject's personal data becoming known to unauthorized persons.

The Norwegian Data Protection Authority has noted that Elgiganten A/S has tightened the procedures for processing personal data for employees and supplemented the warehouse's burglary prevention measures when installing a roof. The Danish Data Protection Authority must make sure that Elgiganten A/S ensures that the applicable procedures are complied with and that they continuously monitor this.

3.2. Summary

The Danish Data Protection Authority finds that there are grounds for expressing serious criticism that Elgiganten A/S' processing of personal data has not taken place in accordance with the rules in the data protection regulation article 32, subsection 1.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free exchange of such data and on the repeal of Directive 95/46/EC (general regulation on data protection).