Complaint about security breach at Falkonergårdens Gymnasium and HF

Date: 18-10-2021

Decision

Public authorities

Criticism

Complaint

Notification of breach of personal data security

Treatment safety

The Norwegian Data Protection Authority has criticized the fact that Falkonergården had not reported a security breach to the authority. The Norwegian Data Protection Authority also found no basis for overriding the school's assessment of what were appropriate security measures.

Journal number: 2021-32-2067.

Summary

The Danish Data Protection Authority has made a decision in a case where a student at Falkonergården complained that the school mistakenly sent a written warning in connection with excessive absences to another student. The error occurred when an employee entered an incorrect social security number when sending via e-Boks. It was subsequently established that information about the complainant's absence rate was known to others at the school.

The Danish Data Protection Authority expressed criticism that Falkonergården had not met the requirement that breaches of personal data security must be reported to the Danish Data Protection Authority as a starting point.

In the assessment, the Danish Data Protection Authority emphasized that Falkonergården had not proved that it was unlikely that the incident entailed a risk to the complainant's rights. This could, for example, be damage to the complainant's reputation.

The Danish Data Protection Authority also found no basis for overriding Falkonergården's assessment of what were appropriate security measures.

In this connection, the Danish Data Protection Authority emphasized that this was a one-off case, that only a few trusted employees sent the letters in question, that the management often emphasized to these employees the importance of entering the correct social security number and that the individual employee always double-checks the social security number.

However, the Danish Data Protection Authority called on Falkonergården to reconsider their measures in the event of any repeat cases.

Decision: The Data Protection Authority hereby returns to the case where [complainant] (hereafter complainant) on [date] 2021 has complained that Falkonergården Gymnasium and HF (hereafter Falkonergården) have passed on the complainant's personal data to unauthorized persons.

1. Decision

After a review of the case, the Data Protection Authority finds that there is a basis for expressing criticism that Falkonergården's processing of personal data has not taken place in accordance with the rules in the data protection regulation[1] article 33, subsection 1.

The Danish Data Protection Authority also finds that there is no basis for stating that Falkonergården's processing of personal data has occurred in violation of Article 32, paragraph 1 of the Data Protection Regulation. 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 the complainant is a student at Falkonergården and that on [date] 2021 the school sent a written warning by mistake with the complainant's absence information and the complainant's full name to another student at the school.

Falkonergården made the complainant aware of the situation on the same day and apologized for the mistake.

2.1. Falkonergården's remarks

Falkonergården has stated that the unauthorized disclosure happened when a secretary had to prepare letters with notice of neglect to several students. The letters contained information about the student's absenteeism rate and a warning that the student would be expelled from the school if attendance did not improve. In the process of sending, the secretary mistakenly forgot to change the social security number when the letter was sent to e-Boks through the school's electronic student archive.

Falkonergården has also stated that only a few trusted employees send information to e-Boks, and the management has regularly emphasized to these employees the importance of entering the correct social security number. The employees who work with student information, including sending to e-Boks, are very aware of the type of information they work with. The employees are fully aware of the importance of the correct information being sent to the correct recipient. In this connection,

Falkonergården has stated that the individual employee always double-checks that shipments via e-Boks are made to the correct social security number.

Falkonergården has argued that sending to e-Boks is always done by manually entering the social security number. Falkonergårde therefore did not have the opportunity to implement technical measures that ensured against this type of incident.

Falkonergården has stated that the school has requested the recipient to delete the letter and remain silent about the content. Falkonergården has also asked for confirmation that the recipient has deleted the information.

Furthermore, Falkonergården has stated that the management has made it strict for employees who send to e-Boks that when preparing and sending several letters in the same work process, in the future they must start anew with each letter, and not start from a previous letter . Employees who send to e-Boks will in future ensure that they are extra careful every time information is sent via e-Boks, and make sure that it is the correct recipient that is sent to.

Falkonergården has considered whether the school can take technical measures that can ensure that similar incidents do not happen in the future. The school is not aware of such measures that can remedy human errors such as entering the wrong social security number.

Falkonergården has stated that the school has not reported the incident as a breach of personal data security to the Danish Data Protection Authority, as the school found, on the basis of a risk assessment, that it was unlikely that the incident would or could involve a risk to the complainant's rights or freedoms, even if the complainant is young. Falkonergården has, however, for good measure informed complaints about the incident.

Falkonergården has also assumed that the relevant information in the erroneously forwarded document is not covered by Article 9 of the Data Protection Regulation, and that there is also no information of a confidential nature in the document.

In the decision not to report the incident to the Danish Data Protection Authority, Falkonergården has further emphasized that the content of these warnings to students with excessive absences are standard letters, in which nothing appears other than a recommendation to the student to reduce the absence and the consequences of not heed the warning. Combined with the risk assessment, it was assessed that the complainant's rights would not be harmed or endangered in any way.

Falkonergården has argued that it appears from previous decisions from the Data Protection Authority that it is the sensitivity of the information that is important for the handling of the type of information and in which cases the authority should be

notified.

Finally, Falkonergården has stated that the assessment of not making a report to the Data Protection Authority was made based on which category of information was in the forwarded letter, and that the wrong recipient was another student at Falkonergården.

2.2. Complainant's comments

The complainant has stated that there has been a security breach which Falkonergården should report to the Danish Data Protection Authority. Complainant has also stated that [complainant] is very affected by the situation, as rumors about [complainant's] absenteeism rate abound at school.

3. Reason for the Data Protection Authority's decision

The Danish Data Protection Authority assumes that there has been a breach of personal data security (unauthorized disclosure of personal data), as Falkonergården has mistakenly sent information about a written warning to the complainant due to excessive absences and the complainant's absence percentage to another student.

3.1.

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. This includes, among other things, that as the data controller you must ensure that information about the registered person does not come to the knowledge of unauthorized persons.

The Danish Data Protection Authority is of the opinion that it will normally be an appropriate security measure that only a few trusted employees - after having been properly instructed - can use the manual transmission of documents in e-Boks. This requires that there is an appropriate check of the entered social security number before the shipment takes place.

The Danish Data Protection Authority assumes that only a few trusted employees send information via e-Boks, that the management regularly emphasizes to these employees the importance of entering the correct social security number and that the individual employee always double-checks that sending via e - Box is made to the correct social security number.

On this background, and since there is no further documentation of precedent, the Danish Data Protection Authority finds no basis for overriding Falkonergården's assessment that the measures are appropriate in relation to the described risks.

The Danish Data Protection Authority therefore has no basis for stating that Falkonergården's processing of personal data has

taken place in violation of Article 32, paragraph 1 of the Data Protection Regulation. 1.

The supervision must, however, emphasize that repeated cases must cause the data controller to reconsider his measures, this could possibly be that the check of the social security number must be carried out by a person other than the person who entered it, or that workflows are considered that copy the information in question from an authoritative source e.g. the student's birth certificate or similar.

3.2.

In the event of a breach of personal data security, the data controller must report the breach to the Danish Data Protection Authority in accordance with Article 33, paragraph 1 of the Data Protection Regulation. 1. Notification must not be made, however, if it is unlikely that the breach of personal data security entails a risk to the rights or freedoms of the data subject.

The Danish Data Protection Authority finds that Falkonergården – by not reporting the breach to the Danish Data Protection Authority – has not met the requirements of the Data Protection Regulation, Article 33, subsection 1, which gives the inspectorate reason to express criticism.

In this connection, the Danish Data Protection Authority has emphasized that all breaches of personal data security must, as a matter of principle, be reported to the Danish Data Protection Authority, and that it is only if it is unlikely that the breach of personal data security entails a risk to the rights or freedoms of natural persons that be notified.

In this connection, the Danish Data Protection Authority is of the opinion that Falkonergården has not proved that it is unlikely that the breach of personal data security entails a risk to the complainant's rights or freedoms. A risk to the rights and freedoms of natural persons includes, among other things, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data subject to confidentiality or any other significant economic or social disadvantage for the data subject.

Furthermore, the Danish Data Protection Authority is of the opinion that information on the percentage of absences and information that a person has received a warning due to excessive absences is confidential information.

The Danish Data Protection Authority also finds that the fact that the wrong recipient of the information was another student at Falkonergården cannot lead to a different assessment of whether a report should be made to the Danish Data Protection Authority. In this connection, the Data Protection Authority has emphasized that precisely because it was a different student, information subsequently appeared about the complainant's absence rate at school.

The Danish Data Protection Authority must enforce that Falkonergården reports similar security breaches to the Danish Data

Protection Authority in accordance with the data protection regulation's article 33, subsection 1.

4. Concluding remarks

In conclusion, the Danish Data Protection Authority must state that in this case Falkonergården does not have to make a separate notification of the breach of personal data security, cf. the data protection regulation, article 33, subsection 1. In this connection, the Danish Data Protection Authority has emphasized that the breach is sufficiently explained in connection with the handling of the case by the Danish Data Protection Authority.

[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).