Criticism of the Correctional Service for not clarifying a possible breach in time

Date: 31-05-2023

Decision

Law enforcement authorities

Criticism

Reported breach of personal data security

Notification of breach of personal data security

The Danish Data Protection Authority has made a decision in a case where the Norwegian Prison and Probation Service became aware of information about a possible breach, but failed to investigate the incident quickly to clarify whether it was a breach of personal data security.

Journal number: 2021-816-0292

Summary

The Danish Data Protection Authority has made a decision in a case where a group of employees at the Norwegian Correctional Service created a closed Messenger group on Facebook, where official communication took place between employees in Storstrøm Prison about both inmates in the prison and employees at the Norwegian Correctional Service.

The Probation Service received several inquiries from an employee with a concern that there had been a breach of personal data security, as work-related communication took place in the closed Messenger group. Despite the inquiries, the Norwegian Correctional Service did not investigate the case until 6 months after receiving the first inquiry.

The Norwegian Data Protection Authority has expressed criticism of the Danish Prison and Probation Service for not having investigated the possible breach quickly with a view to clarifying whether it was a breach of personal data security and, by extension, for not having reported the breach to the Norwegian Data Protection Authority in a timely manner - that is, without undue delay and if possible no later than 72 hours after the Norwegian Correctional Service became aware of the breach.

When is the data controller considered to be aware of a breach?

The Danish Data Protection Authority is of the opinion that the data controller is generally considered to be aware of a breach when an employee of the data controller becomes aware of the breach. If the data controller is in doubt as to whether there has been a breach of personal data security, the presumption that a breach may have occurred should lead to the data

controller investigating the incident in more detail with a view to clarifying whether a breach has actually occurred breach of personal data security. The investigation must take place as soon as possible, and the data controller must determine with a reasonable degree of certainty whether a breach has taken place and whether the incident must be reported to the Danish Data Protection Authority.

Decision

The Danish Data Protection Authority hereby returns to the case, where the Norwegian Correctional Service reported a breach of personal data security on 4 August 2021 with follow-up on 23 August 2021. The reviews have the following reference numbers:

4812ec25ed13684f4e82aa5840f8dce19183b364

and

67d0ed7b92be23ab889b0efec25ebea8d1d7c636

1. Decision

After a review of the case, the Danish Data Protection Authority finds that there is a basis for criticizing the fact that the Norwegian Correctional Service's processing of personal data has not taken place in accordance with the rules in section 28 of the Law Enforcement Act. 1.[1]

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

2. Case presentation

The Norwegian Probation Service reported a breach of personal data security to the Danish Data Protection Authority on 4 August 2021. The Norwegian Probation Service subsequently sent a follow-up on 23 August 2021 and a statement in the matter on 13 October 2021.

It then appears from the case that, in March/April 2020, a staff group at the Correctional Service created a closed Messenger group (hereafter the group) on Facebook, where official communication took place between employees of Storstrøm Prison about both inmates in the prison and employees at the Correctional Service.

The Norwegian Correctional Service has informed the case that, on 11 November 2020, an employee informed the management at Storstrøm Prison via e-mail that the employee had been invited to a Messenger group by the staff group in question, and that the employee sought advice from the management as to whether the employee should join the group. The

employee doubted whether it was against the applicable rules to communicate via Messenger.

On the same day, the management informed the employee that the management cannot interfere in the establishment of such groups in private auspices with a social agenda. At the same time, the management stated that it is not permitted to use external systems for case processing.

On the same day, in a new e-mail to the management, the employee expressed concern about whether the communication in the group took place exclusively in private, or whether information that the employees had come into possession of as part of their work was also shared. The employee's manager stated that the manager was not himself in some groups to ensure that work-related communication took place via the right channels. The manager then considered the case closed and took no further action.

In this connection, the Norwegian Correctional Service has acknowledged that on 11 November 2020 there were indications that official communication took place in the group. Furthermore, the Norwegian Correctional Service has stated that they have assessed that the management's great focus on the cooperation problems in the unit could be a reason why the indications were not given greater value.

On 9 April 2021, the same employee again informed the management at Storstrøm Prison that information about inmates was being shared in the group. The employee then – at the management's request – sent screenshots of parts of the content in the group.

Based on the inquiry, the prison's management contacted the area's data protection and information security officer on 12 April 2021. The Norwegian Correctional Service has stated that at this time they were not aware that this constituted a breach of personal data security.

Furthermore, the Correctional Service has stated that the employees were encouraged to close the group and delete the correspondence in April 2021, which is why it has not been possible to investigate the scope further. On an unspecified date in April, the personnel group confirmed to the management that the Messenger group was closed.

It also appears from the information in the case that the Correctional Service's whistleblower scheme received an inquiry on 22 June 2021 from the employee in question, who had alerted the management to the possible sharing of work-related information in November 2020, regarding the sharing of information in the group.

The Norwegian Prison and Probation Service has stated that it was still not clear to them that there was a breach of personal

data security until early August 2021, after which the Norwegian Prison and Probation Service reported the incident as a breach of personal data security to the Norwegian Data Protection Authority on 4 August 2021.

3. Reason for the Data Protection Authority's decision

The Danish Data Protection Authority assumes, on the basis of the information provided by the Norwegian Prison and Probation Service, that the management at Storstrøm Prison already became aware on 11 November 2020 that an employee was concerned about whether information that the members of the group had received was shared in the Messenger group knowledge of at work, and that there were therefore indications that there had been a breach of personal data security.

3.1. Section 28 of the Law Enforcement Act, subsection 1

It follows from Section 28, subsection 1 of the Law Enforcement Act that, in the event of a breach of personal data security, the data controller must report the breach to the supervisory authority without undue delay and, if possible, no later than 72 hours after the data controller has become aware of the breach, unless it is unlikely that the breach entails a risk to the rights of natural persons.

In this connection, the Danish Data Protection Authority is of the opinion that the data controller is generally considered to be aware of a breach when an employee of the data controller becomes aware of the breach. If the data controller has doubts that there has been a breach of personal data security, the presumption that a breach may have occurred should lead to the data controller investigating the incident in more detail with a view to clarifying whether a breach has actually occurred breach of personal data security. The investigation must take place as soon as possible, and the data controller must determine with a reasonable degree of certainty whether a breach has taken place and whether the incident must be reported to the Danish Data Protection Authority.

On the basis of the above, the Norwegian Data Protection Authority finds that the Norwegian Prison and Probation Service – by not having investigated the incident quickly and, by extension, notifying the Norwegian Data Protection Authority of the breach in a timely manner – has not acted in accordance with the rules in section 28, subsection of the Law Enforcement Act.

1.

The Danish Data Protection Authority has emphasized that an employee of Storstrøm Prison already on 11 November 2020 notified the prison's management of the potential breach of personal data security, and that the Norwegian Prison Service did not, in this connection, conduct an investigation into the potential breach, which would have enabled the Norwegian Prison

Service to report the breach of personal data security to the supervisory authority in a timely manner.

The fact that the management's focus on cooperation problems in the unit may have been a reason why the information about a possible breach was not investigated does not change the above assessment.

The Danish Data Protection Authority must note that the Norwegian Prison and Probation Service only reported the breach of personal data security on 4 August 2021 after the management had been notified of the incident on several occasions.

[1] Act on the processing of personal data by law enforcement authorities. Act No. 410 of 27 April 2017 as amended by Act No. 503 of 23.5 2018 and Act No. 506 of 23.5 2018.