e-Boks receives criticism for not having adequate security in e-Boks Express

Date: 03-03-2022

Decision

Private companies

Criticism

Supervision / self-management case

Unauthorized access

Treatment safety

Data processor

After becoming aware that it was possible to access another user's profile when logging in to e-Boks Express, the Data Protection Authority started a case of self-management against e-Boks. The supervisory authority has now made a decision in the case, and the decision illustrates, among other things, that login – regardless of whether it is with NemID – does not protect data if the rights the user gets after logging in are not correct

Journal number: 2021-431-0138

Summary

The Danish Data Protection Authority was informed in March 2021 that it was possible to access someone else's user's profile by logging in to e-Boks Express.

In April 2021, the Danish Data Protection Authority therefore started a case of self-management against e-Boks.

E-boks Express is a self-service portal where companies can send messages and documents.

An error in Nets' setup of the user validation of NemID meant that when a user accessed e-Boks Express by logging in with NemID Business/NemID employee signature with key card, access could be established to other companies' information and information about documents sent in e -Box Express.

E-Boks claimed that NemID is used in e-Boks Express to ensure that only the persons authorized by the sending company have access to e-Boks Express.

The Danish Data Protection Authority expressed criticism that e-Boks had not met the requirement for appropriate security measures, because e-Boks had not tested all relevant usage scenarios when logging in to e-Boks Express.

The Norwegian Data Protection Authority stated in this connection that a login is used to identify the user who uses the IT solution – in this case e-Boks Express.

After login, the rights a user is given must ensure that the access to data is exactly what this user must have access to. E-Boks should thus have discovered during testing that e-Boks Express gave access to other users' data, even if the user identification failed.

The decision illustrates, among other things, that login – regardless of whether it is with NemID – does not protect data if the rights the user gets after logging in are not correct.

1. Decision

After a review of the case, the Danish Data Protection Authority finds that there is a basis for expressing criticism that e-Boks' processing of personal data has not taken place in accordance with the rules in the data protection regulation 0F[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 inquiry of 22 March 2021 from a user of e-Boks Express that when he had to log on to e-Boks Express on 22 March 2021, he instead went directly to another user's profile. On 9 April 2021, the user informed the Danish Data Protection Authority that the same thing happened on 9 April 2021 when he clicked on "Login to e-Boks Express".

Brugen contacted e-Boks Express by telephone on 22 March 2021 about the problem.

It also appears from the inquiry that it immediately appeared that the user could send messages to e-Boks from other users' profiles.

2.1. E-box's comments

Initially, e-Boks has stated that e-Boks Express is a new online self-service portal where small and medium-sized companies can register as senders and send messages/documents securely to e-Boks' end-users' digital mailboxes. It is not possible for the sending company to receive messages/documents in e-Boks Express. A sending company only has the option to send messages/documents and subsequently see the self-selected title of sent messages/documents and the time of sending.

E-Boks has argued that NemID Erhverv/NemID employee signature is used in e-Boks Express to ensure that only the persons authorized by the sending company have access to e-Boks Express.

E-Boks has stated that it has inadvertently been possible for the person who has approached the Danish Data Protection Authority to access the company information of another sending company, i.e. the name of the company, the name of the contact person, the company's address and CVR no. It has also been possible to access the heading and date of a sent document. In this connection, e-Boks has stated that it has not been possible for the sending company to access information about the recipient of the document, just as it has not been possible to access the content of the sent message.

In addition, e-Boks has stated that sending companies can only access e-Boks Express via NemID Erhverv/NemID employee signature, i.e. with key file, key card or key app. That it was possible for the mentioned sending company to access another user's account was due to an error in Nets Danmark A/S' (hereafter Nets) setup of the user validation of NemID Business/NemID employee signature. The error related only to the use of key cards. E-Boks has stated that e-Boks has been in dialogue with Nets, who have confirmed that the error in the setup has been corrected.

Finally, e-Boks has stated that e-Boks has run tests on the error correction, thus verifying that the error has been corrected, so that similar incidents cannot occur.

2.2. Nets' remarks

Initially, Nets stated that E-Ident is a broker solution that is used to identify persons and companies.

Nets has stated that the error only affected people who used NemID key cards associated with companies and who also used e-Boks Express. It was thus not a general NemID error and affected a small number of users who used e-Boks Express in that period.

In addition, NemID has stated that in E-Ident it is registered in logs how many people are logged on to e-Boks Express with a key card. The number of logins with key cards was 227 in March 2021 and 28 in April 2021. This is a proportion of these that potentially had the opportunity to exploit the error.

Nets has stated that the company cannot get the number closer than that 304 people could potentially have exploited the error, as Nets cannot distinguish between whether a person has logged on to e-Boks Express with a NemID key card as an employee or as a private person. The error only affected people with a NemID key card who logged in as an employee, which is an unknown proportion of the 304 logged-in people.

Nets has also stated that the error was in a so-called "sub" field, which contains the name of the ID type - in this case NemID with key card - and the unique CVR and RID values, where the RID number indicates an employee's unique identification. For

NemID key cards, the reading of the CVR and RID numbers from the user's NemID in relation to e-Boks Express failed, and the value was therefore set to zero, for those persons who, during the period of the incident, used a physical NemID key card associated with a company, and who in same period used e-Boks Express.

It appears from Net's statement that the error correction consisted in the code being updated so that the reading of CVR and RID values worked correctly, and these values could be entered correctly in the "sub" field in relation to e-Boks Express.

Regarding the duration of the security breach, Nets has stated that the error first occurred on 4 March 2021, when e-Boks, as data controller, contacted Nets. Nets was then in ongoing dialogue with e-Boks about the first error identification and later how the error could be corrected. The error was fixed in production at Nets on April 27, 2021.

3. Reason for the Data Protection Authority's decision

On the basis of what was disclosed to the case, the Danish Data Protection Authority assumes that an error in Net's setup of the user validation of NemID meant that when a user accessed e-Boks Express by logging in with NemID Business/NemID employee signature with key card, it could be established access to the company information of other sending companies and the title of sent documents and the time of sending.

On this basis, the Danish Data Protection Authority assumes that there has been unauthorized access to 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.

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 Danish Data Protection Authority is of the opinion that the requirement cf. Article 32 for adequate security will normally mean that changes to existing IT solutions and development of new solutions should only take place with due focus on processing security - both in connection with development and testing of the solution.

Based on the above background, the Danish Data Protection Authority finds that E-Boks - by not having tested all relevant usage scenarios when logging into E-Boks Express with NemID Business/NemID employee signature with key card - has not

taken appropriate organizational and technical measures to ensure a security level that matches the risks involved in E-Boks' processing of personal data, cf. the data protection regulation, article 32, subsection 1.

The Danish Data Protection Authority has emphasized that E-Boks is seen to have based its security on the fact that a login with NemID had been established, even though it did not protect against unauthorized access to data. In particular, the authority has attached importance to the fact that testing must also uncover the possible error scenarios in the selected log-on component, in the specific case, the possibilities that existed for having different implementations of NemID with the users.

The Danish Data Protection Authority notes in this connection that a login is used to identify the user who uses the IT solution. After login, the rights a user receives must ensure that access to data is exactly what this user must have access to. E-Boks should thus have discovered during testing that e-Boks Express gave access to other users' data, even if the user identification failed.

After a review of the case, the Danish Data Protection Authority finds that there is a basis for expressing criticism that E-Boks' 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 mediating response, the Danish Data Protection Authority emphasized that the breach did not provide the opportunity to see information other than the contact person, company name, the self-selected title of sent messages and documents and the time of sending.

In addition, the Danish Data Protection Authority emphasized that exploiting the error could only take place after logging in with NemID Business/NemID employee signature with key card, which – although this could not prevent the possibility of abuse – would nevertheless give users the impression that they might be exposed , if they exploited the vulnerability and that this could potentially deter them from doing so. In addition, only customers who used e-Boks Express could take advantage of the error, which limited the number of people who could discover and abuse it.

[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).