Serious criticism: Non-compliance with the principle of data protection through design at LB Forsikring A/S

Date: 27-06-2022

Decision

Private companies

Serious criticism

Notification of breach of personal data security

Treatment safety

Basic principles

The Danish Data Protection Authority expresses serious criticism in a case where customers of LB Forsikring A/S have had unauthorized access to documents and e-mails in their own claims cases from the insurance company's car claims department.

Journal number: 2021-441-10244

Summary

LB Forsikring A/S' archiving system was designed with a setting that meant that e-mails were for a period associated with a claims case with read rights depending on which domain it was sent from. In practice, this meant that all documentation that was identified with the same claim number - and that was sent from several widespread mail providers - became visible on the customer's "My page". The documents could, among other things, be from counterparties, witnesses and auto mechanics, and contained personal data such as contact information, witness statements, payment information – and in at least one case a social security number. LB Forsikring A/S has estimated that there were a maximum of 340 documents and that a similar number of registered persons may have been affected.

Before the implementation of the filing system in 2019, LB Forsikring A/S had prepared an implementation plan that contained several tests. The tests should, among other things, ensure that documents were assigned the correct document ID and were placed correctly, but the setting in question was not identified in the test run.

The Danish Data Protection Authority determined that – in addition to the use of all the recognized test forms – already from the development of the system's business processes and design, it is the duty of the data controller to ensure an effective implementation of the data protection principles by building this into the system support, so that it provides the necessary

guarantees in the processing of personal data and meets the requirements of the General Data Protection Regulation (GDPR).

When developing a portal solution such as LB Forsikring A/S' archiving system, where access must be given to stored documents with personal data in them, it is not in accordance with the current technical level if a mail domain is only given weight according to which documents are given access to. In addition, it will be part of the current technical level that the data controller incorporates follow-up controls that ensure that such an automatic process alone provides the correct access.

Since LB Forsikring A/S neglected to accommodate this in the actual design of the solution, even before the processing was organised, the basic principle of integrity and confidentiality was not respected.

Against this background, the Danish Data Protection Authority expresses serious criticism of LB Forsikring A/S.

1. Decision

After a review of the case, the Data Protection Authority finds that there are grounds for expressing serious criticism that LB Forsikring 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 and Article 25, subsection 1.

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

2. Case presentation

LB Forsikring A/S, hereafter ("LB"), reported a breach of personal data security on 30 September 2021. On 5 October 2021, LB sent a follow-up notification to the Data Protection Authority.

It appears from the case that members of LB have had unauthorized access to documents and e-mails from the car claims department for a period from 21 February 2019 to 7 October 2021. The insurance company became aware of this when a customer stated that he had access to the department's correspondence with a counterparty in his ongoing claims case.

LB has informed the case that their portal solution facilitates communication between the case handlers and the members when signing a policy and handling claims. Members can access the "My page" page by logging in with NemID and find out about policies, any claims, upload documents and contact the insurance company.

It appears from the case that all documentation that is visible on the member's "My page" is assigned a document ID. In the case at hand, LB's archiving system has allocated all e-mails from the following domains - {hotmail.dk - hotmail.com - outlook.com - outlook.dk - gmail.com - gmail.dk - icloud.com - mme.com - private. dk} – a document ID which – as a starting point – has been set to make the content visible on the member page – regardless of the fact that these came from a third

party and did not concern the member. On that basis, all documentation from the e-mail domains in question was classified as sent by the member.

LB has informed the case that the error has its origins in the implementation of the insurance company's portal solution in 2019. LB states that the technical settings, including the setting of the classification of certain email domains with a certain document ID, were due to human error.

It appears from the case that the incident only concerns the car damage department. It is only e-mails from a third party that are identified with the claim number, which is the member's claim case, that have potentially been visible on "My Page". Members have not had unauthorized access to other members' claims. The personal data in the documents that have been accessed by mistake have been names, contact details, social security numbers, payment details, IP addresses and witness statements, and the registered; customers, witnesses, injured parties and counterparties.

LB has informed the case that the incident has been going on for 959 days from 21 February 2019 to 7 October 2021, when the insurance company shut down the visibility of the document ID in question. The log shows that 3,923 documents have been opened during this period. LB has carried out a sample of 645 of these documents, which showed that in a specific case a member had unauthorized access to other people's documents in 56 cases. Based on their manual review, LB has estimated that a maximum of 340 documents, and a corresponding number of registered ones, may be affected by the incident.

LB has further informed the case that, before the implementation of the portal solution in 2019, they had drawn up an implementation plan. The implementation plan included several tests of the solution, including ensuring that documents were assigned the correct document ID and were correctly placed. According to LB, the mentioned error was not identified on the grounds that it was not a systemic error. LB did not do any sampling, including to review the material content as well as the sender of emails prior to implementation. LB states that it was the actual setting and assignment of the document ID to the e-mail domains in question, "which was inappropriate and posed a small risk that e-mails from third parties regarding a particular member's claim case would also become visible on the member's "My page"." LB acknowledges that with the technical equipment in question there is an inherent risk of members gaining unauthorized access to other people's personal data.

It appears from the case that LB continuously updates the portal solution in order to improve it and ensure sufficient security measures, as required by the Data Protection Act. According to LB, the e-mails in question have not been discovered, since

the portal contains a large amount of documents and information, of which the e-mails constitute only a small fraction. LB states that it would have required a human review of "My Page" to identify the error. LB does not carry out such a check.

LB has implemented prior organizational measures in the form of instructing the case handlers to react if they become aware of incorrectly placed information on the portal and otherwise when contacted by members. LB has reportedly not had any internal reports since the security breach occurred. In addition, LB continuously assesses which documents must be visible on "My page" to ensure confidential information. LB has stated that – on the basis of this case – they will examine the process for assigning document IDs and document types, including to ensure that the automated process for assigning document IDs does not result in a repeated security breach.

LB has stated that those registered are injured parties, counterparties, witnesses and car mechanics. The content of the documents and e-mails in question do not predominantly contain confidential information. The random check also showed a limited amount of personal data, including information that had often already been exchanged between the parties. The manual review showed that, by far, only ordinary personal data such as name and e-mail appeared. In a few cases, an injured party's account number, an invoice, a claim number and the like appeared. In one out of 56 cases, an injured party's contact form was found, from which a social security number appeared. LB has not notified the registered.

3. Reason for the Data Protection Authority's decision

Based on what LB provided, the Danish Data Protection Authority assumes that the injured party in the period from 21 February 2019 to 7 October 2021 had unauthorized access to the personal data of other parties in connection with their own car damage case. On this basis, 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 Danish Data Protection Authority is of the opinion that the requirement in Article 32 for adequate security will normally

mean that in systems with a large amount of information about a large number of users, higher requirements must be placed on the diligence of the data controller in ensuring that unauthorized access does not occur to personal data, and that all probable error scenarios should be tested in connection with the implementation of new software where personal data is processed.

Furthermore, the Danish Data Protection Authority is of the opinion that a technical setting that automatically determines the visibility of documents with personal data and where access to this is solely determined by which e-mail domain the sender uses, especially when these are domains that are frequently used by private individuals as well as businesses, does not is an expression of adequate security, cf. the data protection regulation, article 32, subsection 1.

Based on the above, the Danish Data Protection Authority finds that LB – by not having introduced ongoing measures to check and correct the settings of the portal solution system for the visibility of documents – has not taken appropriate technical and organizational measures to ensure a level of security that suits the risks that are in the data controller's processing of personal data, cf. the data protection regulation, article 32, subsection 1.

3.2. Article 25 of the Data Protection Regulation

This follows from the data protection regulation's article 25, subsection 1, that the data controller - both at the time of determining the means for the processing and at the time of the processing itself - must take appropriate technical and organizational measures, which are designed for the effective implementation of data protection principles and for the integration of the necessary guarantees in the processing to meet the requirements of this regulation and protect the rights of data subjects.

It is the opinion of the Danish Data Protection Authority that, in 2019, LB did not take appropriate technical and organizational measures through design in order to meet the requirements of the data protection regulation when determining the digitization of the business processes, the implementation and the layout of their portal solution system, in which information about natural persons was to be processed.

The Danish Data Protection Authority has placed particular emphasis on the fact that the development of portal solutions that create access to stored documents containing personal data cannot be said to reflect the current technical level, if the mail domain's suffix is given weight in isolation when granting access. In addition, it will normally be part of the current technical level that built-in follow-up controls, with appropriate follow-up frequency, ensure that such an automated process only

provides correct access.

Knowing, already at the time of the organization of the treatment, to have neglected this, and by using the email domain as a factor, in the access to personal data and as it should have been countered by the design of the solution, to ensure compliance with the basic principle in Article 5, paragraph . 1, letter f on integrity and confidentiality (as well as Article 32), LB has not observed Article 25, paragraph 1.

After a review of the case, the Danish Data Protection Authority finds that there are grounds for expressing serious criticism that LB's processing of personal data has not taken place in accordance with the rules in the data protection regulation, article 32, subsection 1 and Article 25, subsection 1.

When choosing a response, the Danish Data Protection Authority emphasized that LB, prior to the initial implementation of the portal solution in 2019, carried out a flawed risk assessment in the layout of their system. This has meant that the security breach has lasted 959 days and the measures previously implemented by LB were insufficient. It also appears that LB was aware of the risk of accidental confusion of parties to the case and visibility of documentation.

In addition, the Danish Data Protection Authority has emphasized that the scope of the processing of personal data must be considered significant by an insurance company and that certain data subjects should enjoy special protection and confidentiality, including e.g. witness in a car damage case according to the compensation. Finally, the Danish Data Protection Authority has emphasized that LB has not taken a position on the risk profile of whether some of the data subjects have address or name protection.

In a mitigating way, the Danish Data Protection Authority has placed emphasis on the fact that the personal data has generally been information that was already known to the person – who gained the unauthorized access.

The Danish Data Protection Authority notes that LB intends to investigate the process for assigning document IDs and document types in the future, including to prevent a similar security breach in the future.

3.3. Summary

The Danish Data Protection Authority finds grounds for expressing serious criticism that LB Forsikring A/S' processing of personal data has not taken place in accordance with the rules in the data protection regulation, article 32, subsection 1 and Article 25, 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).