Complaint about lack of encryption

Date: 02-07-2019

Decision

Private companies

In a specific case concerning the encryption of e-mails, Lowell Danmark A / S had carried out a risk assessment, in which the procedure was assessed as an appropriate security measure by the Danish Data Protection Agency.

Journal number: 2019-31-1263

Summary

The Danish Data Protection Agency has processed a complaint in which a citizen has complained that Lowell Danmark A / S has sent confidential information about the citizen unencrypted over the Internet.

On 26 June 2019, the Danish Data Protection Agency made a decision in the case. In the opinion of the Danish Data Protection Agency, Lowell Danmark A / S 'processing of the information about the citizen had taken place in accordance with Article 32 (1) of the Data Protection Ordinance. 1.

The decision should be seen as a concrete reasoned example that a data controller can use an opportunistic TLS 1.2 encryption (encryption on the transport layer that only works if the recipient's server supports it) when transmitting confidential information over the Internet if the data controller a risk assessment has correctly assessed that such a setup constitutes an appropriate precautionary measure.

In the specific case, Lowell Danmark A / S had emphasized, among other things, that generally only a few of their recipients use very old e-mail client versions or service providers, where an e-mail will be sent unencrypted, and that they specifically assess this for the individual recipients. The e-mails in question were, incidentally, sent encrypted on the transport layer for complaints.

According to the information in the case, the Danish Data Protection Agency had no basis for overriding the risk assessment made by Lowell Danmark A / S, and assumed that the technical and organizational measures in the situation were appropriate.

In the opinion of the Danish Data Protection Agency, Lowell Danmark A / S had thus, on the basis of a risk assessment, implemented appropriate security measures, cf. Article 32 of the Data Protection Ordinance.

Decision

The Danish Data Protection Agency hereby returns in the case, where X on 5 January 2019 and 19 January 2019 complained to the Danish Data Protection Agency about Lowell Danmark A / S 'processing of information about this. The Danish Data Protection Agency must initially note that the Authority has not taken a position on this decision on whether Lowell Danmark A / S has consented to communicate with X via e-mails, as Chapter II of the Data Protection Ordinance [1] does not set requirements for the data controller's method choice. communication with data subjects, including whether the communication is to take place by physical mail or digitally.

Decision

After a review of the case, the Danish Data Protection Agency finds that Lowell Danmark A / S 'processing of X's personal data has been in accordance with Article 32 (1) of the Data Protection Ordinance. 1.

Below is a more detailed review of the case and a justification for the Danish Data Protection Agency's decision.

2. Circumstances of the case

It appears from the case that on 5 January 2019 and 19 January 2019, Lowell Danmark A / S sent information about outstanding arrears to X's e-mail. It also appears from the case that Lowell Danmark A / S in the transmission of the e-mails in question has used a - so-called - TLS 1.2 encryption (encryption on the transport layer) based on the algorithm AES256 and that this has been done with the setting called opportunistic (which sends mails encrypted during transport to the recipient if supported but unencrypted if not supported).

3. Comments of the parties

3.1. Your comments

X has stated that on 5 January 2019 and 19 January 2019, Lowell Denmark sent information about X's arrears to his e-mail (e-mail address) via an unencrypted connection. X has further stated that he does not believe that he has given permission for Lowell Danmark A / S to contact him via e-mail.

3.2. Lowell Danmark A / S comments

Lowell Danmark A / S has denied that the two e-mails were sent via an unencrypted connection.

Lowell Danmark A / S has stated that the transmissions of the e-mails in question have been in accordance with the risk assessment that the company has carried out pursuant to Article 32 of the Data Protection Ordinance. In this connection, the company has emphasized that case numbers are used in the e-mails in question. e-mails, and that these are an expression of

a pseudonymisation of personal data, and that the risk of the information coming to the knowledge of unauthorized persons is low. The company has also emphasized that e-mails are only sent to debtors who have actively approved the use of e-mails for communication with Lowell Danmark A / S. In the assessment, Lowell Danmark A / S has emphasized that in general only a very small number of their recipients use very old e-mail client versions or service providers, where an e-mail will be sent unencrypted, and the specific assess this for the individual recipients.

Lowell Danmark A / S has stated that all e-mails sent from the company - as a minimum - are sent with Opportunistic Transport Layer Security (TLS) 1.2 using all the latest cipher suites that Office365 supports. The cipher suite used in sending the mentioned e-mails to X has been "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384". It has also been noted by the company that X's email domain supported Opportunistic TLS.

Lowell Danmark A / S has finally stated that the sending of the two e-mails took place on the basis that X - in connection with a telephone bailiff court meeting on DATE. MONTH YEAR - has orally given permission for this, and that the company has not registered any kind of inquiry from X, where the latter has refused this form of inquiry. Lowell Danmark A / S has further stated that X has now been deregistered from this service, as on the basis of the complaint to the Danish Data Protection Agency, the company is of the opinion that he no longer wishes to be registered for this.

4. Legal rules

Article 32 (1) of the Data Protection Regulation 1, states that the data controller, taking into account the current technical level, the implementation costs and the treatment nature, scope, coherence and purpose, as well as the risks of varying probability and seriousness of natural persons' rights and freedoms, implement appropriate technical and organizational measures to ensure a level of security appropriate to these risks.

The provision of Article 32 (1) of the Data Protection Regulation 1, contains an obligation for the data controller to protect both sensitive information and confidential and general non-sensitive information, just as the data controller must ensure that the data controller's systems, organization and procedures are arranged so that the requirements of Article 32, para. 1, complied with.

The Danish Data Protection Agency is of the opinion that it would normally be an appropriate security measure - for both public and private actors - to use encryption when transmitting confidential and sensitive personal data via the Internet.

5. Decision

After a review of the case, the Danish Data Protection Agency finds that Lowell Danmark A / S 'processing of X's personal data has taken place in accordance with Article 32 (1) of the Data Protection Ordinance [2]. 1. The Danish Data Protection Agency has hereby emphasized the information provided by Lowell Danmark A / S that a risk assessment has been carried out, where the specific procedure is deemed to be an appropriate guarantee that opportunistic TLS was used in the transmissions of the e-mails in question. 1.2 encryption based on AES256, that X's e-mail client supported this form of encryption and that the 2 sent e-mails have been encrypted on the transport layer.

The Danish Data Protection Agency notes that the Authority in general - when processing e-mail with sensitive and / or confidential information - encourages the data controller to set up his mail server to enforce TLS (Forced TLS), at least in version 1.2. However, in the Authority's view, it is not - in itself - contrary to Article 32 of the Data Protection Regulation to use an opportunistic TLS if the controller has - on the basis of a risk assessment - correctly - assessed that such a setup constitutes an appropriate security measure.

In the specific case, the Danish Data Protection Agency has not found any evidence that could override the risk assessment carried out by Lowell Damnark A / S, in relation to the use of encryption.

In the specific case, however, the Danish Data Protection Agency must emphasize that a risk assessment cannot be based on what the data subject himself has given permission for, as such acceptance cannot be equated with which level of security is appropriate.

Concluding remarks

Lowell Danmark A / S is today informed of this decision.

The Danish Data Protection Agency hereby considers the case closed and does not take any further action in the case.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General data protection regulation).

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General data protection regulation).