Complaint about treatment safety

Date: 07-10-2019

Decision

Private companies

On the basis of a complaint, the Danish Data Protection Agency has assessed that the use of the encryption form opportunistic TLS without further control in a specific case was not a sufficient security measure.

Journal number: 2019-331-0135

Summary

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

In a previous decision (j.nr. 2019-31-1263), the Danish Data Protection Agency has decided that the security measures Lowell - in the specific case - had taken on the basis of their risk assessment were appropriate. The use of opportunistic TLS was supplemented with a check of whether the recipient domain supported TLS and it appeared from the risk assessment that in cases where the recipient domain could not receive TLS, a form of communication other than e-mail was used.

The significant difference from the previous decision was that in this case Lowell had not been able to verify whether the recipient domain could receive TLS, and despite this lack of verification, sent the e-mail with opportunistic TLS 1.2, in addition, Lowell could not prove whether e- the mail was actually received encrypted.

Therefore, in this case, where it has not been proven that the recipient domain will be able to receive emails encrypted with TLS, Lowat finds that Lowell has not been able to demonstrate that the processing has taken place in a way that ensures sufficient security for the personal data in question, including protection against unauthorized access to personal data, using appropriate technical or organizational measures, in accordance with Article 5 (2) of the Data Protection Regulation; 2, cf. Article 32 (1) (f) 1 and 2.

Decision

The Danish Data Protection Agency hereby returns to the case, where [complainants] on 22 March 2019 complained to the Authority that Lowell Danmark A / S had sent confidential information about complaints, including information about social security numbers and the complainants' arrears, unencrypted over the Internet.

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 complaints via e-mails, as Chapter II of the Data Protection Ordinance [1] does not set requirements for the data controller's choice of method. communication with the data subject, including whether the communication is to take place via e-mail or via a secure website.

Decision

After a review of the case, the Danish Data Protection Agency finds that there are grounds for expressing criticism that Lowell Danmark A / S 'processing of personal data has not taken place in accordance with the rules in Article 5 (1) of the Data Protection Ordinance. 2, cf. Article 32 (1) (f) 1 and 2.

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

2. Case presentation

2.1. Complainant's remarks

Complainants have generally stated that on 22 March 2019, Lowell Danmark A / S sent confidential personal information about complaints, including information about social security numbers and arrears, to the complainant's personal e-mail via an unencrypted connection.

Complainants have further stated that he does not believe that he has given permission for Lowell Danmark A / S to contact him via e-mail.

2.2. Lowell Danmark A / S 'comments

Lowell Danmark A / S has generally denied that the e-mail was sent via an unencrypted connection.

Lowell Danmark A / S has stated that the transmission of the e-mail in question has been in accordance with the risk assessment that the company has carried out pursuant to Article 32 of the Data Protection Regulation.

Lowell Danmark A / S has further 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 relevant e-mail for complaints has been "TLS_ECDHE_RSA_WITH_ AES_256_GCM_SHA384". Lowell Danmark A / S has finally stated that they have investigated whether the complainant's e-mail supports TLS 1.2, and that the investigation showed that it was not possible to ascertain whether the complainant's e-mail supports TLS 1.2.

Justification for the Danish Data Protection Agency's decision

The Danish Data Protection Agency assumes that Lowell Danmark A / S 'sending of the e-mail in question of 22 March 2019 to complaints containing confidential information about complaints has been sent with an opportunistic set TLS 1.2 with cipher suite TLS_ECDHE_RSA_WITH_AES _256_GCM_SHA384. The Danish Data Protection Agency also assumes that the investigation carried out by Lowell Danmark A / S did not make it possible to establish whether the complainant's e-mail supported TLS 1.2.

The Danish Data Protection Agency has in an earlier decision (the Authority's j.nr. 2019-31-1263) found that opportunistic TLS on the basis of a risk assessment, which included an assessment of whether the recipient domain could receive TLS in a given version and where the mail could be received encrypted, in the specific case could constitute an appropriate technical security measure.

In this case, where it has not been proven that the recipient domain will be able to receive emails encrypted with TLS, the Danish Data Protection Agency finds that Lowell Danmark A / S has not been able to demonstrate that the processing has taken place in a way that ensures sufficient security for the personal information. , including protection against unauthorized access to personal data, using appropriate technical or organizational measures, in accordance with Article 5 (2) of the Data Protection Regulation. 2, cf. Article 32 (1) (f) 1 and 2.

The Danish Data Protection Agency has hereby emphasized that Lowell Danmark A / S has not been able to establish that the complainant's e-mail address to which the e-mail was sent supports shipment with TLS 1.2, and that it is a matter of transmission of confidential personal information.

Against this background, the Danish Data Protection Agency finds that there is a basis for expressing criticism that Lowell Danmark A / S 'processing of personal data has not taken place in accordance with the rules in the Data Protection Ordinance, Article 5 (1). 2, cf. Article 32 (1) (f) 1 and 2.

[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).