Risk assessment when disclosing personal information

Date: 05-03-2020

Decision

Private companies

Following three reported breaches of personal data security, the Danish Data Protection Agency has taken a more detailed position on processing security and requirements for risk assessments.

Journal number: 2019-441-3399

Summary

The Danish Data Protection Agency has dealt with three cases in which BroBizz A / S has reported that in connection with the company's response to customer inquiries, personal information - including information about location - was passed on to unauthorized persons.

On the basis of the reported breaches, the Danish Data Protection Agency asked, among other things, BroBizz submits their risk assessment for customer verification and a series of copies of the company's specific procedures and instructions, including in particular regarding the identity of natural persons requesting insight.

On the basis of the risk assessment, the Danish Data Protection Agency finds that the company, in assessing which security level is appropriate, has not taken sufficient account of the risks posed by the processing, e.g. by unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.

Decision

On 20 September, 29 November and 12 December 2019, the Danish Data Protection Agency received three notifications from BroBizz A / S (hereinafter BroBizz) about breaches of personal data security (respectively the Authority's j.nr. 2019-441-3399, 2019-441-4055 and 2019-441-4160).

Decision

After reviewing the cases, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that BroBizz 'processing of personal data has not taken place in accordance with the rules in Article 32 (1) of the Data Protection Regulation [1]. 1 and Article 32, para. 2.

The Danish Data Protection Agency also finds grounds for ordering BroBizz to make an assessment of the risks to the data

subjects associated with the type of processing of personal data that the company carries out in connection with securing the identity of the natural person who makes a request as referred to in Articles 15 to 21 of the Regulation, in accordance with Article 32 (2). 2.

The risk assessment must include a mapping of the risk to the data subjects' rights and then a balancing of these risks in relation to the measures taken to protect these rights [2].

The order is issued pursuant to Article 58 (1) of the Data Protection Regulation. 2.

The deadline for compliance with the order is 4 weeks from today's date. The Danish Data Protection Agency must request to receive a copy of the risk assessment in question no later than the same date.

According to the Data Protection Act [3] § 41, para. 2, no. 5, is punishable by a fine or imprisonment for up to 6 months for anyone who fails to comply with an order issued by the Danish Data Protection Agency pursuant to Article 58 (1) of the Data Protection Regulation. 2, letter d.

In addition, the Danish Data Protection Agency finds that BroBizz 'processing of personal data has taken place in accordance with Article 33 (1) of the Data Protection Regulation. 1 and Article 34, para. 1.

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

On September 20, 2019, BroBizz reported a breach of personal data security.

It appears from the notification that BroBizz on 17 September 2019 at 17:43 became aware that a customer service employee on 13 September 2019 had handed over personal information about a customer, including information about location, to unauthorized persons.

In this connection, BroBizz stated, among other things, following:

“Customer service employee hands over telephone location data (regarding the use of BroBizz transmitter) to a person other than the customer. It's about Person A (the customer) and person B (girlfriend of the customer). Person B informs person A's telephone number, and based on this, person A is searched in our customer system, and information about 2 passages is confirmed to person B. Subsequently [on 17 September 2019], person A contacts BroBizz A / S and states that they are ex-girlfriends, and that person A did not request this information was disclosed to person B. "

Brobizz further stated that on September 20, 2019, the customer service manager contacted the affected customer by telephone and notified of the incident.

On 24 October and 5 November and 12 December 2019, BroBizz issued additional statements to the case.

By e-mail of 24 October 2019, BroBizz sent, at the request of the Danish Data Protection Agency, a copy of the company's risk assessment regarding "general verification of customers". The risk assessment was signed on 6 August 2019.

The risk assessment submitted shows that the risk of employees processing customer inquiries without verification is “very small”, which is the lowest probability that the company works with.

It also appears that the "consequence for you as a customer" is that "customer information is provided to the wrong customer / non-customer". In addition, it appears from the risk assessment that the preventive action with a view to preventing and minimizing risks is that "employee follows instructions / process". In conclusion, it appears from the risk assessment - under "outcome of preventive action / reason for approved index" - that "data is not handed out / processed to the wrong person / customer".

By letter dated 5 November 2019, BroBizz issued a supplementary statement to the case. Brobizz stated in this connection that the company had prepared a process for general verification of customers, one for verification of customers in connection with personal data inquiries and an instruction. The company further stated that the said procedures had not been complied with in the case in question.

BroBizz further stated that various employees have undergone e-learning since May 25, 2018, and that customer service employees are introduced to relevant personal data law issues in connection with the start of their employment. Continuing education has taken place on an ad hoc basis.

At the request of the Danish Data Protection Agency, BroBizz sent by letter dated 11 December 2019 a number of copies of the company's specific procedures and instructions, including in particular the identity of the natural person making a request as referred to in Articles 15-21, cf. Article 12 (1) of the Data Protection Regulation . 6.

It appears from the company's internal instructions ("BBAS - Verification of Customers in BBAS") that customers must provide two customer-specific information based on a list of four types of information that must ensure that the customer is verified before the inquiry is processed in the usual way. In relation to customer inquiries where a request is made, which deals with the data subject's rights under the Data Protection Regulation, BroBizz has established instructions (“BBAS - GDPR

verification of customers”). It appears from this that the customer by telephone inquiry is requested to make his inquiry in writing, and that the team leader verifies the customer on the basis of the customer's submitted information before submitting a reply. Similar safety measures appear from e.g. BroBizz's Information Security Policies.

BroBizz has finally stated that it has been emphasized to the customer service employee in question that the transmission of information must take place using the company's internal processor, and that relevant employees have been further instructed in how internal instructions under the Data Protection Regulation are to be complied with in the future.

2.2

By letter dated 29 November 2019, BroBizz has reported another breach of personal data security.

It appears from the notification that BroBizz on 27 November 2019 became aware that a customer service employee on 15 November 2019 - at the request of ForSea Helsingborg AB on behalf of Customer A - by mistake updated Customer A's e-mail address with Customer B's e e-mail address, and subsequently sent a new code to the updated e-mail address, after which Customer A had access to Customer B's account.

In this connection, BroBizz has stated:

ForSea Helsingborg AB contacts BroBizz A / S on behalf of one of their customers A in order to change the customer A's email address at Brobizz A / S. Brobizz A / S and customer A have entered into an agreement to issue an Autobizz which can be used to pay for ferry crossings. In connection with updating customer A's email address, ForSea Helsingborg AB also requests that customer A be sent a new password to Brobizz A / S "My Account". As Forsea meets BroBizz's internal requirements for customer verification, the employee updates what he believes is customer A's account with the new email address. However, a manual error occurs here as the Brobizz employee updates another customer's account with customer A's email address. Then a new code is sent to the updated email address, after which customer A has access to the other customer's "My Account". "

BroBizz has further stated that the company will notify the registered person, and has been in contact with Customer A and asked him to delete any. stored information.

BroBizz has further stated that it has been emphasized to the customer service employee that there may only be one customer image open at a time.

2.3

By letter dated 12 December 2019, BroBizz has reported a further breach of personal data security.

It appears from the notification that BroBizz on 11 December 2019 at 11:15 became aware that a customer service employee on 27 November 2019 updated Customer A's e-mail address under Customer B's customer number, after which Customer A could access Customer B's BroBizz profile.

In this connection, BroBizz has stated, among other things, following:

"Customer A contacts on 26 November 2019 via a form in BroBizz IT system where he requests an update of the email address on a customer number which he allegedly thinks is his own but turns out to be Customer B's customer number. In this connection, BroBizz's internal validation procedure will not be complied with as BroBizz will not be provided with a minimum of two pieces of information that can verify the customer, after which the customer service employee will update the e-mail address under the wrong customer number on 27 November 2019. Customer A then orders a new password which is sent to the just updated email address. After this, customer A can log in to Customer B's account, which he does and updates the associated credit card on 11 December 2019 to his own credit card. Later in the day on 11 December, the error is found and Customer B's account is blocked so that only Customer B can log in. After this, Customer B is contacted by telephone and informed about the process and he is asked to update his payment card, which means that Customer B can see Customer A payment card in limited condition. Customer A also states that on 11 December 2019 he himself contacted Customer B in order to clarify the matter (this is confirmed by Customer B by telephone). In addition, Customer A shows up at the reception in order to open his Brobizz. "

BroBizz has further stated that the company has been in contact with both affected customers, just as the customers themselves have been in contact with each other, which is why it is assessed that no notification should be given to the affected persons.

BroBizz has further stated that only one employee in the company's customer service will process these inquiries in the future. In addition, all customers will in future contact via e-mail, after which correct verification can be performed.

Justification for the Danish Data Protection Agency's decision

3.1 Article 32 (1) of the Data Protection Regulation 1

The Danish Data Protection Agency assumes that BroBizz on 13 September, 16 November and 27 November 2019 - due to lack of security and confirmation of the identity of the natural person who made a request as referred to in Articles 15-21 -

passed on personal data, including .a. location information, about three customers to outsiders.

It follows from Article 12 (1) of the Data Protection Regulation 6, that, without prejudice to Article 11, the data controller may, if there is reasonable doubt as to the identity of the natural person making a request as referred to in Articles 15 to 21, request additional information necessary to verify: the identity of the data subject.

It further follows from Article 32 (1) of the Data Protection Regulation 1, that the data controller must take appropriate technical and organizational measures to ensure a level of security that is appropriate to the risks involved in the data controller's processing of personal data. In the Data Inspectorate's view, this means, among other things, that the data controller must ensure that information about data subjects does not come to the knowledge of unauthorized persons.

The Danish Data Protection Agency finds that BroBizz 'processing of personal data has not taken place in accordance with the rules in Article 32 (1) of the Data Protection Regulation. BroBizz has not complied with the requirement to implement appropriate organizational security measures to ensure the identity of the natural person making a request within the meaning of Articles 15 to 21 of the Regulation.

In this connection, the Danish Data Protection Agency has emphasized that the same type of incident has occurred three times within a short time. The Danish Data Protection Agency finds that the cases are an indication that BroBizz's internal procedures and instructions are either not sufficient or that the employees are not sufficiently aware of this.

The Danish Data Protection Agency has further emphasized that there is insufficient education and training of employees in data protection, including processing security. The measures that have reportedly been taken, namely that various employees have completed one course since 25 May 2018, that employees in customer service are introduced to relevant personal data law issues in connection with the start of their employment, and that the ongoing training takes place on ad hoc basis, are in the opinion of the Data Inspectorate not sufficient. This is confirmed by the fact that Brobizz in two and a half months has passed on information to unauthorized persons in three cases.

In addition, the Danish Data Protection Agency has emphasized that personal information about location is covered by one breach of personal data security, which entails a relatively high risk to the data subject's rights, as exposure of the information may involve, for example, breach of privacy for the person concerned.

On this basis, the Danish Data Protection Agency finds that BroBizz has not taken appropriate organizational and organizational measures to ensure a level of security that matches the risks involved in the company's processing of personal

data, cf. Article 32 (1) of the Data Protection Regulation. 1.

3.2. Article 32 (1) of the Data Protection Regulation 2

Article 32 (1) of the Regulation Paragraph 2 states that in assessing the appropriate level of security, particular account shall be taken of the risks posed by processing, in particular in the event of accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or stored. or otherwise treated.

The risk assessment must thus be based on risks to natural persons (the registered persons), and not e.g. risks to the data controller (legal entities), in this case BroBizz.

The Danish Data Protection Agency finds that the copy of a risk assessment submitted by BroBizz does not appear to include an assessment of what risks a disclosure to unauthorized persons may pose to customers' rights and freedoms. The Danish Data Protection Agency finds that the document only deals with the incident itself and does not affect possible risks for the data subjects' rights, especially exemplified in that the document states that the consequence for the customer is that "info is disclosed to a wrong customer".

The Danish Data Protection Agency may, for example, mention identity theft as possible risks. In addition, location information can have extremely unpleasant consequences for the data subject in the hands of people with malicious intent, for example in cases of harassment or stalking. In this connection, the Danish Data Protection Agency may note that in one case information about the location of a customer's ex-girlfriend has been passed on.

In addition, the Danish Data Protection Agency lacks documentation of how BroBizz has arrived at the assessed consequences and probabilities, including special documentation of how BroBizz has concluded that the probability of employees processing customer inquiries without verification is assessed as "very small". The Danish Data Protection Agency finds this problematic, especially considering that this has happened in three cases within a short time. The Danish Data Protection Agency can therefore not agree with BroBizz's assessment that the risk of employees treating customer inquiries without verification as "very small".

In addition, the Danish Data Protection Agency also does not find that it can be described as a sufficiently clear preventive action that “employees follow instructions / process”. The Authority finds this preventive action extremely unclear.

Against this background, the Danish Data Protection Agency finds that BroBizz - in assessing the appropriate level of security - has not taken into account in particular the risks posed by the processing, in particular in the event of accidental or unlawful

destruction, loss, alteration, unauthorized disclosure or access to personal data. , transmitted, stored or otherwise processed in accordance with Article 32 (2) of the Regulation. 2.

3.3. Article 33 (1) of the Data Protection Regulation 1 and Article 34, para. 1

The Danish Data Protection Agency finds that BroBizz - by reporting the incidents in question to the Authority without undue delay and, if possible within 72 hours after the company became aware of this - has acted in accordance with Article 33 (1) of the Data Protection Regulation. 1.

The Danish Data Protection Agency further finds that BroBizz - by notifying the affected customers in the Authority's cases with j. 2019-441-3399 and 2019-441-4055 - have acted in accordance with Article 34 (1) of the Data Protection Regulation. In this connection, the Danish Data Protection Agency has emphasized BroBizz's information that a manager in the department in one case, among other things, has contacted one of those affected by telephone and that in the second case BroBizz will notify the customer whose information is covered by the incident.

In addition, the Danish Data Protection Agency agrees with BroBizz's assessment in the Authority's case with j. No. 2019-441-4160 that there is no high risk to the rights and freedoms of the persons concerned, therefore no notification should be made. In this connection, the Danish Data Protection Agency has emphasized BroBizz 'information that the company has been in contact with both affected customers and that the customers have been in contact with each other.

On this basis, the Danish Data Protection Agency finds that BroBizz has acted in accordance with the rules in Article 33 (1) of the Data Protection Regulation. 1 and Article 34, para. 1.

3.4. The Data Inspectorate's conclusion

In summary, the Danish Data Protection Agency finds that there are grounds for expressing serious criticism that BroBizz 'processing of personal data has not taken place in accordance with the rules in Article 32 (1) of the Data Protection Regulation. 1 and Article 32, para. 2.

The Danish Data Protection Agency also finds grounds for ordering BroBizz to make an assessment of the risks to the data subjects associated with the type of processing of personal data that the company carries out in connection with securing the identity of the natural person who makes a request as referred to in Articles 15 to 21 of the Regulation, in accordance with Article 32 (2). 2.

The risk assessment must include a mapping of the risk to the data subjects' rights and then a balancing of these risks in

relation to the measures taken to protect these rights. [4]

The order is issued pursuant to Article 58 (1) of the Data Protection Regulation. 2.

The deadline for compliance with the order is 4 weeks from today's date. The Danish Data Protection Agency must request to receive a copy of the risk assessment in question no later than the same date.

According to the Data Protection Act, section 41, subsection 2, no. 5, is punishable by a fine or imprisonment for up to 6 months for anyone who fails to comply with an order issued by the Danish Data Protection Agency pursuant to Article 58 (1) of the Data Protection Regulation. 2, letter d.

In addition, the Danish Data Protection Agency finds that BroBizz 'processing of personal data has taken place in accordance with Article 33 (1) of the Data Protection Regulation. 1 and Article 34, para. 1.

Concluding remarks

The Danish Data Protection Agency expects a copy of the risk assessment in question no later than 4 weeks from today.

The Danish Data Protection Agency has taken note of BroBizz's comments that the company has taken a number of measures in order to comply with the data protection rules.

In conclusion, the Danish Data Protection Agency must note that BroBizz - on the basis of the mapping of the risk to the data subjects' rights - must take / implement appropriate security measures with a view to reducing / eliminating the identified risks for the data subjects.

[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] For further guidance, please refer to the Danish Data Protection Agency and the Council for Digital Security's Guidance text on risk assessment: https://www.datatilsynet.dk/media/7900/vejledende-tekst-om-risikovurder.pdf

[3] Act No. 502 of 23 May 2018 on supplementary provisions to the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Act).

[4] For further guidance, please refer to the Danish Data Protection Agency and the Council for Digital Security's Guiding text on risk assessment: https://www.datatilsynet.dk/media/7900/vejledende-tekst-om-risikov appeared.pdf