DATATILSYNET

Ascio Technologies
Ørestads Boulevard 108, 10. th.
2300 København S

Sent by Digital Post

18. juni 2020

J.nr. 2019-7320-1443
Dok.nr. 226402
Sagsbehandler
[redacted]

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

CVR 11883729

Complaint about the processing of personal data

The Danish Data Protection Agency hereby reacts to the case where [redacted] (hereinafter 'the complainant') on 30 August 2018 wrote to the Information Commissioner's Office (ICO) regarding Ascio Technologies, Inc. Denmark (hereinafter 'Ascio') processing of personal data.

In accordance with Article 56 of the GDPR[1], the Danish DPA has been designated as the lead supervisory authority in the case.

1. Decision

Following a review of the case, the Danish DPA considers that there are grounds to **criticise** the fact that the processing of personal data by Ascio has not been carried out in accordance with the rules set out in Article 32(1), Article 5(1)(a) and Article 33(1) GDPR.

Below is a closer look at the case and a justification for the DPA's decision.

2. Facts

It appears from the file that the complainant — through the company Sanktuary Group — sent an email on 15 August 2018 to Ascio, where he draws attention to the fact that e-mails with illegal content are sent from the domain name finance-invoies.net.

Ashcio has stated that the domain belongs to Ascio, but that the domain is managed via OWEEX, which is an authorised Ascio distributor.

On 18 August 2018, Ascio sent the e-mail of the complainant to OWEEX and asked the distributor to take measures in relation to the phishing activities. On 30 August 2018, the distributor informed Ascio that finance-invoices.net had already been deactivated on 14 August 2018 and that the illegal activity had thereby ended. On 4 September 2018, Ascio informed the complainant that the company had handled the complaint and that finance-invoices.net had been deactivated.

In the case Ascio stated, that it is the company's normal procedure for dealing with potential domain use to contact the distributor who has direct contact with the domain owner, so that

[1]European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons 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).

they can deal with any abuse. This is usually done without passing the contact information. Ascio further stated that it was an error that the personal data of the complainant was not communicated in an anonymous form.

On 26 September 2018, the complainant informed Ascio that data about him had been disclosed to unauthorised parties. Ascio answered the letter of the complainant on the same day and apologized for the fact that the company had disclosed personal data about him to OWEEX, who is responsible for the contact with the owner of finance-invoices.net.

2.1. The comments made by Ascio

In the case Ascio stated that the company has now emphasized their pre-existing internal guidelines for handling personal queries in order to ensure that a similar incident will not happen again.

However, Ascio did not request OWEEX to remove the email with the data of the complainant.

In addition, Ascio has stated that, since the complainant's email was sent only to a trusted distributor, and therefore not to the owner of a finance-invoices.net, Ascio considered that it was not necessary to notify the Danish DPA of the breach, given that the incident did not involve a significant risk of the rights and freedoms of the complainant.

3. Justification for the decision of the Danish Data Protection Authority

The Danish DPA finds that, by passing personal data of the complainant to the distributor, OWEEX, Ascio has failed to comply with Article 32(1) of the GDPR.

The Danish DPA also considers that, by failing to request OWEEX to delete the email in question, Ascio has failed to comply with Article 5(1)(a) of the GDPR.

Finally, the Danish DPA finds that Ascio did not act in accordance with Article 33(1) GDPR to notify the data breach to the Danish DPA.

For this reason, the Danish DPA considers that there are grounds to **criticise** the fact that the processing of personal data by Ascio has not been carried out in accordance with the rules set out in Article 32(1), Article 5(1)(a) and Article 33(1) of the GDPR.

In its assessment, the Danish DPA has taken into account the statement made by Ascio **that** the disclosure of the data about the complainant was an error and contrary to the company's guidelines, **and** that it is usually not necessary for the company to transmit contact information when the company contacts the distributor for potential domain misuse.

The Danish DPA has further taken into account, **that** it is the authority's view that, in accordance with the principle of fairness under Article 5(1)(a), the controller must — if personal data has come to his/her knowledge — ensure that the defect or security defect is remedied and seek to limit the harmful effects thereof. For example, in the case of unjustified transfers, the controller must ensure that data is erased or possibly collected or returned from ineligible recipients. As a result, the Danish DPA has attached importance to the fact **that** Ascio did not request OWEEX to delete the email in question.

Finally the Danish DPA has attached importance to the fact **that** all personal data breaches must in principle be notified to the Danish DPA, and **that** it is only if the personal data breach is unlikely to result in a risk to the rights or freedoms of natural persons that there is no need to notify the Danish DPA. A risk to the rights and freedoms of individuals includes, inter alia, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality

of data subject to professional secrecy or any other significant economic or social disadvantage for the data subject.

In the present case, the Danish DPA has attached particular importance to the fact that the transfer took place to an external distributor. For this reason, it cannot be ruled out that the breach in question entails a risk to the rights and freedoms of the complainant. The Danish DPA therefore finds that Ascio should have notified the Danish DPA of the personal data breach.

The Danish DPA emphasizes, that Ascio is not required to notify this particular breach separately, since the breach has been adequately informed in the course of the proceedings of this complaint

However, the Danish DPA emphasizes, that Ascio in the future must notify a breach of security to the Danish DPA in accordance with Article 33(1) GDPR.

The Danish DPA has noted the information provided by Ascio that the company has emphasized their already existing internal guidelines for handling personal communications in order to ensure that a similar incident will not happen again.

4. Final remarks

A copy of this letter will be sent to the ICO to date with information to the complainant, requesting that the ICO forward the letter to the complainant.

The Danish DPA notes that the DPA expects to publish this decision on the website of the DPA.

The Danish DPA hereby considers the case closed and does not take any further action.

The decision of the Danish DPA can be brought before the courts, cf. Section 63 of the Danish Constitution.

Med venlig hilsen

[redacted]

Annex: legal basis

Annex: Legal basis

Extract from European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons 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).

Article 5. Personal data shall be:

a) processed lawfully, fairly and transparently with respect to the data subject (legality, fairness and transparency);
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
d) accurate and, where necessary, kept up to date;every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data were processed;personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

Para. 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

Article 32. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, inter alia, as appropriate:

a) pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Para. 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction,

loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Para. 3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

Para. 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Para. 2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

Para. 3. The notification referred to in paragraph 1 shall at least:

a) describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
c) describe the likely consequences of the personal data breach;
d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Para. 4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

Para. 5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.This documentation must enable the supervisory authority to verify compliance with this Article.

Article 56. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

Para. 2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

Para. 3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter.Within a period of three

weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

Para. 4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply.The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision.The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

Para. 5. Where the lead supervisory authority decides not to hear the case, the supervisory authority which referred the matter to the lead supervisory authority shall examine the case in accordance with Article 61 and 62.

Para. 6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.