Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2021-11-22, no. DI- DI-2021-3398. Only the Swedish version of the decision is deemed authentic.

Ref no:
DI-2021-3398, IMI case no. 61381

Date of decision:
2021-11-22

Date of translation:
2021-11-30

Supervision under the General Data Protection Regulation – Pieces Interactive AB

Final decision of the Swedish Authority for Privacy Protection (IMY)

The Authority for Privacy Protection (IMY) finds that Pieces Interactive AB has processed personal data in breach of Article 32 of the General Data Protection Regulation (GDPR)[1] by failing to take technical measures to ensure a level of security for its contact forms on its websites www.piecesinteractive.se and www.piecesinteractive.de during the period 14 August 2018 to 11 February 2020 that is appropriate in relation to the risks to the rights and freedoms of natural persons arising from the processing.

The Authority for Privacy Protection issues Pieces Interactive AB a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Article 32 of the GDPR.

Report on the supervisory report

The Authority for Privacy Protection (IMY) has initiated supervision regarding Pieces Interactive AB (Pieces or the company) due to a complaint. The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Germany) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in Germany.

The complaint

The complaint states the following. Pieces has contact forms on its websites (www.piecesinteractive.se and www.piecesinteractive.de) which, as of 14 August

[1] Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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).

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

2018, probably transmitted unencrypted information, such as name and e-mail address, that individuals submitted to the company via the contact forms.

What Pieces has stated
Pieces has mainly stated the following.

Pieces is the data controller for the processing to which the complaint relates.

Transfers of data from individuals to Pieces via the contact forms on the company's websites were not encrypted in the period from 14 August 2018 to 11 February 2020. Pieces used the Hypertext Transfer Protocol Secure (HTTPS) protocol for the websites, but it does not appear to have been used on the pages with the contact forms.

Pieces completely removed the contact forms on 19 April 2021 and now only provides an email address for contact. It has new pages that was put into use in on 12 February 2020 and the forms were then encrypted with HTTPS until they were removed.

Pieces estimated that 25-30 transfers has been made through the forms. The types of data processed in connection with such transfers were names, contact details and messages in a free text field. The messages have consisted of internship applications, interview requests from students and the media, as well as various external companies that want to sell services. The information sent has been of a general character and has not contained any sensitive personal data. There has been no possibility to attach files, so for example, no CVs or similar have been transferred through the forms.

These transfers relate to Article 32 of the GDPR on appropriate technical security measures in the sense that Pieces used its content management's system standard message form, where all messages were sent to a specific email address. No messages (including address) have been saved after the end of the communication. Because the forms were was intended only for general contacts with the company, no further consideration was made as to the importance of having an encrypted solution because the personal data that could be assumed to be provided were not sensitive. However, at the time, the company thought that the forms were HTTPS encrypted.

Justification of the decision

Applicable provisions, etc.

Any processing of personal data must comply with the fundamental principles set out in Article 5 of the GDPR. One of these is the requirement of security under Article 5(1)(f). It states that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) makes it clear that the controller must be responsible for and be able to demonstrate compliance with the fundamental principles.

Article 24 governs the responsibility of the controller. Article 24(1) states that the controller is responsible for implementing appropriate technical and organisational measures to ensure and demonstrate that the processing is carried out in accordance with the GDPR. The measures shall be implemented taking into account the nature,

scope, context and purpose of the processing and the risks, of varying probability and severity, to the rights and freedoms of natural persons. The measures shall be reviewed and updated as necessary.

Article 32 sets out the requirements for the safety of the processing. Pursuant to paragraph 1, the controller and the processor shall – 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 risk of varying likelihood and severity for the rights and freedoms of natural persons – implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Pursuant to paragraph 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.

Recital 75 states that when assessing the risk to the rights and freedoms of natural persons, various factors must be taken into account. It mentions, among other things, confidentiality of personal data protected by professional secrecy, data concerning health or data concerning sex life, where personal data of vulnerable natural persons, in particular of children, are processed or where processing involves a large amount of personal data and affects a large number of data subjects.

It follows from recital 76 that the likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk

Recitals 39 and 83 also provide guidance on the more precise meaning of the GDPR's requirements for the security of the processing of personal data.

Assessment of the Authority for Privacy Protection (IMY)

As the data controller Pieces has to take appropriate technical and organisational measures to ensure a level of security appropriate to the risk with processing pursuant to Article 32(1). Pursuant to Article 32(2), in assessing the appropriate level of security, particular account shall be taken of the risks posed by processing, in particular the unauthorised disclosure of, or access to, the personal data processed.

The investigation shows that, during the period from 25 May 2018 to 19 April 2021, Pieces had contact forms on its websites used by individuals to contact the company. Until 11 February 2020, transfers to the company via the forms have been made through an open network and without protection of encryption. Data transmitted has consisted of name, e-mail address and data in a free text field for messages that individuals have chosen to transmit to the company.

IMY notes that an open network, such as the internet, is characterised by the fact that others can access data communicated in the network, such as the transmissions made via the contact form. Since access to the data has been possible though the open network, there has been a high level of exposure to unauthorised persons, with the result that the risk of unauthorised access has increased. The amount of data has been relatively small, the number of transfers relatively few and the data transferred

has not been privacy sensitive. However, since the contact forms has had a free text field, the risk of sensitivity to the nature of the data has increased, since Pieces was not able to control what data was provided there. Pieces has not taken technical measure to encrypt the transfers through the forms, even though it thought it did. Pieces has neither ensured that the measures which it believed it had taken actually had been implemented.

In the light of the above, IMY finds that the company has not taken technical measures to ensure a level of security for its contact forms on the websites www.piecesinteractive.se and www.piecesinteractive.de during the period from 14 August 2018 to 11 February 2020 that is appropriate in relation to the risks to the rights and freedoms of natural persons arising from the processing. The processing has therefore been carried out in violation of Article 32 of the GDPR.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Factors to consider is the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The duration of the infringement has indeed been relatively long, but it has consisted of relatively few transfers of neither sensitive nor privacy sensitive data. The infringement was made due to negligence. Pieces has not previously received any corrective measures for infringements of the data protection rules. Prior to the opening of this supervisory case, Pieces had also corrected the lack of technical measures and, during the processing of the case, has taken further steps regarding the contact forms.

Against this background and the nature of the infringement, IMY considers that it is a minor infringement within the meaning of recital 148 and that Pieces Interactive AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

This decision has been made by Head of Unit [redacted] after presentation by legal advisor [redacted].

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority’s contact information is shown in the first page of the decision.