Datatilsynet

[redacted]

Exempt from public disclosure:
Offl. § 13, jf. personopplysningsloven § 24 første ledd 2. punktum

Your reference	Our reference	Date
	20/03652-12	25.11.2022

Rejection of Complaint and Closure of Case

Introduction

Datatilsynet refers to your complaint received by us on 17 September 2020 regarding SF Anytime AB.

This is a so-called cross-border case. The case is cross-border because SF Anytime AB is a business which is established in more than one member state of the EEA. To ensure consistent practice of privacy legislation in the EU and EEA, European data protection authorities cooperate in the case handling of cross-border cases. The case was entered into the common European case handling system "Internal Market Information System" ("**IMI**").

Progress of the Case

The Swedish data protection authority, Integritetsskyddsmyndigheten ("**IMY**"), has been the lead supervisory authority in the handling of your complaint in accordance with Article 56(1) GDPR. The data protection authorities in Norway, Denmark and Finland have been involved as concerned supervisory authorities, that is they have had the opportunity to provide their opinion and views on the handling and result of the case.

IMY investigated your complaint regarding SF Anytime AB who is the data controller for the relevant processing. IMY concluded that SF Anytime AB had not processed your personal data in breach of the relevant articles of the GDPR, and therefore proposed to close the case.

IMY thereafter uploaded a draft decision to the common European case handling system IMI to give the concerned supervisory authorities, including Datatilsynet in Norway, the opportunity to provide their opinions and views on the handling and result of the case. Neither

Datatilsynet nor the other concerned supervisory authorities had objections to IMYs draft decision, and therefore became bound by it pursuant to Article 60(6) GDPR.

Decision

Datatilsynet adopts the following decision:

The complaint is rejected pursuant to Article 60(8) GDPR.

Please see the attached document for the reasons why your complaint was rejected. The attachment is IMYs draft decision as mentioned above, which Datatilsynet agrees with. The attachment is written in English due to the international co-operation mechanism that had to be used in the handling of the case. Should you wish the attachment to be translated to Norwegian, please contact us.

Right of Appeal

As this decision has been adopted by the NO SA pursuant to Article 56 and Chapter VII GDPR, it is not possible to appeal it before the Norwegian Privacy Appeals Board pursuant to Section 22 of the Norwegian Data Protection Act. This decision may nevertheless be appealed before the Norwegian courts in accordance with Article 78(1) GDPR.

Right to see the case documents

As a party to the case, you have the right to see the case documents pursuant to Section 18 of the Norwegian Public Administration Act. There may however be exceptions in relation to certain types of information pursuant to Section 19 of the Norwegian Public Administraiton Act. Please let us know if you wish to exercise this right.

Kind regards

Tobias Judin
Head of Section

Sebastian Forbes
Senior Legal Advisor

This letter has electronic approval and is therefore not signed

Copy to: SF Anytime AB

Attachment: IMY Draft Decision – SF Anytime AB

Swedish Authority for Privacy Protection

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) draft decision, no. IMY-2022-3576. Only the Swedish version of the decision is deemed authentic.

Ref no:
IMY-2022-3576

Date of draft decision:
2022-09-20

Date of translation:
2022-09-27

Draft decision pursuant to Article 60 under the General Data Protection Regulation – SF Anytime AB

This draft decision is a proposed decision by the Swedish Authority for Privacy Protection (IMY) within the meaning of Article 60 of the General Data Protection Regulation in accordance with the cooperation and coherence mechanisms set out in Chapter VII of the Regulation. The draft is shared with concerned supervisory authorities in a formalized procedure, where they have the opportunity to comment and, where appropriate, raise reasoned and relevant objections to the proposed decision.

This is therefore not a final decision. The justification and the decision may change in whole or in part depending on the outcome of the Article 60 procedure. Following the conclusion of these proceedings, IMY will issue a final decision on the matter.

Decision of the Swedish Authority for Privacy Protection (IMY)

The Authority for Privacy Protection (IMY) finds that the supervision has not shown that SF Anytime AB has processed the complainant´s personal data in breach of Articles 15 and 32 of the General Data Protection Regulation (GDPR)[1].

The case is hereby closed.

Report on the supervisory case

The case handling
The Authority for Privacy Protection (IMY) has initiated supervision regarding SF Anytime AB (the company) due to a complaint. The aim of the supervision has been to investigate if the company has failed in its handling of the complainant's request for access in the manner alleged in the complaint (Article 15 of the GDPR). Further IMY has investigated whether someone has had had unauthorized access to the complainant's personal data and in that case if the company has taken sufficient measures to protect the complainant's personal data from unauthorized access (Article 32 of the GDPR).

[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 he 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

The complaint has been submitted to IMY, in its capacity as responsible supervisory authority under Article 56 of the GDPR. The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Norway) in accordance with the GDPR'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 concerned supervisory authorities have been the data protection authorities in Norway, Denmark and Finland.

The complaint
The complaint mainly states the following. An unauthorized person has had access to the complainant's account on SF Anytime and rented a movie, which resulted in that the complainant´s bank card was debited. The complainant received a receipt of the purchase the 22 of August 2020 and contacted the company on the same day to get access to the IP-address of the person who had accessed his personal data, for the purpose of using the information in a report to the police. The company refused to give the complainant the information. On 25 August 2020 the complainant requested access to all information the company holds about him and was referred by the company by e-mail of 25 August, 29 August and 11 September 2020 to the possibility of downloading the information that the company has concerning him via 'My pages' on the company's website. The complainant downloaded the information but considers that the file does not contain all the information the company has about him.

What the company has stated
The company has stated on 5 July 2022, relevant to the assessment of the complaint, mainly the following.

Concerning unauthorised access
In light of the security measures implemented by the company, the company can conclude that no infringement or attempted infringement has taken place in the company's IT environment during the period in question. Nor has the company received any indication that other customers have been subjected to unauthorised access during the period in question. No one other than the customer who created an SF Anytime account has access to this account or the password created for the account. It is not possible for the company to assess whether an unauthorised person has accessed the complainant's account for reasons beyond the company´s control, for example if the complainant's password has been shared with others, has been stored on an entity shared with others, or if one of receiver unit that the complainant has been using for the service has been handed over, stolen or lost.

According to the company's terms of use, the customer is responsible for protecting login information and passwords so that no one else can access them. In the light of the foregoing, the company's position is that if an unauthorised person had access to the complainant's account it is likely to be due to the fact that it had access to the complainant's login details and passwords.

Request for access
According to the procedure followed by the company at the time, its customers were able to log in to 'My Pages' and download a file containing a copy of all the personal data relating to the customer. Among these data was also the IP address, from which

a movie had been downloaded from, attached. The company states that the complainant has downloaded a file from ‘My Pages’ and has thus been granted access to all the personal data which the company had about the complainant at the time, including the IP address requested.

Justification of the decision

Applicable provisions

Pursuant to Article 15 of the GDPR, the data subject shall have the right to obtain from the controller confirmation of whether personal data concerning him or her are being processed. If such data are processed, the controller shall provide the applicant with additional information and a copy of the personal data processed by the controller.

Article 32 requires the controller and processor to take appropriate technical and organisational measures to protect the complainant’s personal data from unauthorised access.

IMY:s assessment

In the context of this case, IMY has to assess whether anyone has had unauthorised access to the complainant’s personal data and, if so, whether the company has taken sufficient measures to protect the complainant’s personal data from unauthorised access. In addition, IMY has to consider whether the company failed to handle the complainant’s request for access in the manner set out in the complaint, i.e. whether, in the context of the request made, the complainant had access to his personal data, including the IP address requested.

The company has stated that no unauthorised access to the complainant´s account has been obtained by infringement in the company’s IT environment or in any other way that is under the company’s responsibility and control. IMY considers that there has been no reason to question the company’s answer in this regard. Against this background, IMY concludes that the investigation in the case does not show that the company has processed the complainant’s personal data in breach of Article 32 of the GDPR in the manner alleged in the complaint.

As regards the request for access, the company states that the complainant, by the downloaded file from ‘My Pages’, got access to all the personal data which the company had about him at the time, including the requested IP address. IMY also finds no reason, in this regard, to question the company’s answer. IMY therefore concludes that the investigation in the case does not show that the company has processed the complainant’s personal data in breach of Article 15 of the GDPR in the manner alleged in the complaint.

The case will therefore be closed.