Spotify AB

Org. no: 556703-7485

Regeringsgatan 19

111 53 Stockholm

Diary number:

DI-2020-10541

Date:

2021-03-24

Decision after supervision according to

data protection regulation - Spotify AB

The Privacy Protection Authority's decision

The Swedish Privacy Protection Authority states that Spotify AB has processed

personal data in violation of

article 12.4 of the data protection regulation1 by the company in its response of 8 June

2018 on the appellant's objection to the treatment of 24 May 2018 according to

Article 21 has not clearly stated which information

is processed, that the data is processed with the support of a legitimate interest and

what the legitimate interest is and that the answer did not contain information about

the possibility of submitting a complaint to the supervisory authority and requesting

trial.

The Swedish Privacy Protection Authority gives Spotify AB a reprimand according to article 58.2 b

data protection regulation.

Account of the supervisory matter

The Swedish Privacy Protection Authority (IMY) has started supervision of Spotify AB (Spotify

or the company) due to a complaint. The complaint has been handed over to IMY, i

characteristic of the responsible supervisory authority according to Article 56 of the Data Protection Regulation.

The handover has taken place from the supervisory authority in the country where the complainant has left

filed its complaint (Denmark) in accordance with the regulation's provisions on cooperation

in case of cross-border treatment.

Mailing address:

Box 8114

104 20 Stockholm

Website:

www.imy.se

E-mail:

imy@imy.se

Phone:

08-657 61 00

The complaint essentially states the following. The appellant previously had an account and a

paid subscription to the company's music service. The appellant has repeatedly requested that

the company must delete his card details. According to the company, the complainant registered via

PayPal and the company therefore do not process the complainant's card details. The appellant

disputes this, as the appellant's son has been denied registration for one

free trial period where the complainant's card details were used, with the justification that

the card has already been used.

Spotify AB has essentially stated the following.

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 flow of such data and on

repeal of Directive 95/46/EC (General Data Protection Regulation).

The complainant has requested deletion of their credit or debit card details. Spotify however, does not process card details when a user pays via PayPal, such as the appellant done, but instead processes unique identifiers for the payment cards or "instrument" ("unique payment instrument identifier") used by a customer at registration of free trials. The legal basis for the processing is legitimate interests. That the appellant wrote that he withdraws his consent can be interpreted as an objection to the processing. The further processing is not subject to the right to erasure because Spotify has a strong, legitimate interest to continue the treatment that outweighs the rights and freedoms of the complainant.

To sign up for a free trial, potential customers must provide Spotify payment card details that will be used for invoicing when the free trial period has expired. To prevent abuse of them free trial periods that the company offers use the company's unique payment instrument identifier. This means that the same payment instrument cannot used several times. Without this feature, it would be easy for a customer to start new free Spotify accounts for additional trials each time their free trial period expires, by varying information such as email address, and thereby fraudulently exploiting Spotify. The unique payment instrument identifier is a alphanumeric chain generated by Spotify's payment processor PayPal. The enables the unique identification of credit cards, but it does not contain credit card number or other card details. Spotify can't get through

the payment instrument identifier get access to payment card details via

backwards construction (so-called reverse engineering). This process is PCI compliant

DSS2.

The processing is necessary for Spotify to prevent fraud. This is both

a legitimate interest in Spotify and the company's broad customer base, because the company does not

could continue to offer free trial periods of the company's service if

fraud could not be countered in this way. It is also in the public domain

legitimate interest.

Spotify has responded to the complainant's requests but has not deleted the data since

the right to erasure is not applicable. The company responded on 7 December 2017 to

the appellant's original request of 6 December 2017 and 8 June 2018 at

the appellant's latest request of 24 May 2018 and thus within the deadline i

data protection regulation. Regarding the complainant's letter of 15 March 2018

did the company not interpret it as a request for erasure according to the data protection regulation,

but answered the letter on 4 May 2018. The company has informed in several of these answers

the complainant that the company does not store his payment card details and that the company does not

could delete the payment instrument reference that identifies that his card already has

used to take part in one of the company's offers or services.

Regarding what information was provided to the complainant on 8 June 2018 with

the reason for his objection, Spotify considers that the company responded to the complainant

question by explaining that it does not store any card details but only uses one

algorithm to see if a credit card has been used to take part in a Spotify offer

earlier. If the company had reason to believe that the complainant wanted more details

if these categories of personal data had been provided by the company. When the company's

customer service advisers communicate with users, the company always tries to

provide the information that users ask for in a format that is relevant

PCI DSS stands for Payment Card Industry Data Security Standard and is a generally accepted set of guidelines and routines aimed at optimizing security around the use of credit and debit cards.

for the users and also as someone who does not know the provisions of the data protection regulation would understand. Since the appellant neither mentioned the regulation or asked for the legal basis for the processing, the company went did not go into legal details in his answer such as the company's balancing of interests. In addition had the company in its privacy policy communicated to its users that on request happy to provide more information about the balance of interests that the company has made to rely on legitimate interest as a legal basis and informed of the possibility to submit complaints to the regulatory authorities. Furthermore, it should be considered that the case was started more than five months before the data protection regulation entered into force and that the only correspondence that took place in the time after was the company's reply two weeks later then. Since then, the company's customer service advisers have undergone additional training in how they should answer users in a clear and unambiguous way, which questions should be considered such as requests according to the data protection regulation and which questions should forwarded to the company's data protection team and data protection representative. Finally it will taken into account that the company receives over 11,000 customer service cases daily. Although the company's customer service receives continuous training in data protection, the human factor can sometimes lead to a case being answered as a customer service case instead of a response to one the request according to the data protection regulation referred to in article 12.4, especially when the user does not mention personal data or the data protection regulation in his

communication with the company.

The proceedings have taken place through an exchange of letters. Against the background that it applies
cross-border treatment, IMY has used the mechanisms for cooperation
and uniformity found in Chapter VII of the Data Protection Regulation. Affected
supervisory authorities have been the data protection authorities of Portugal, Belgium, Cyprus,
Austria, France, Germany, Slovakia, Italy, Spain, Denmark, Norway and
Finland.

Justification of decisions

The Swedish Privacy Protection Authority's assessment

Has the company had the right to continue processing the complainant's data after
appellant objected to the treatment?

According to Article 17.1 c of the data protection regulation, the data subject shall have the right to
personal data controller without undue delay have their personal data deleted and
the personal data controller shall be obliged to delete without undue delay
personal data if the data subject objects to the processing in accordance with article
21.1 and there is no justified reason for the treatment that weighs more heavily. According to article
21.1 the data subject shall, for reasons relating to his or her specific
situation, have the right to object at any time to the processing of
personal data concerning him or her based on Article 6.1 f. The
the personal data controller may no longer process the personal data unless he or she
can demonstrate decisive justified reasons for the treatment that outweigh it
registered interests, rights and freedoms.

The appellant's letter of 24 May 2018 can be understood as an objection to
the treatment under Article 21(1), for reasons relating to his specific situation on
in such a way that it means that the card number cannot be reused to register new ones
free trial periods of the company's services. Because the request had not been handled

the company has demonstrated decisive justified reasons for the treatment that outweigh
the data subject's interests, rights and freedoms.
In order for processing to be based on Article 6.1 f, all three conditions must be met
prescribed therein are fulfilled, namely, firstly, that the
personal data controller or third party has a legitimate interest (legitimate interest),
secondly, that the processing is necessary for purposes relating to the legitimate
the interest (necessary) and thirdly that not the interests of the data subject or
fundamental rights and freedoms weigh more heavily and require the protection of
personal data (balancing of interests).
The company has stated, among other things, that the company's legitimate interest in the processing is
to counter fraud regarding free trial periods. In recital 47
the data protection regulation states that such processing of personal data which is
absolutely necessary to prevent fraud constitutes a legitimate interest of the person concerned
personal data controller. IMY therefore considers that the company has a legitimate interest.
Furthermore, IMY considers that the processing is absolutely necessary for purposes related to it
justified interest. The investigation shows that the information has been minimized
to the extent that it is possible for the company to be able to achieve the purpose relating to it
justified interest.
In the balancing of interests that must be done between the company's legitimate interest and
the complainant's interests, rights and freedoms, IMY notes that the company's rightful

interest weighs heavily. The treatment appears to be something that the appellant is reasonably capable of

expect upon registration a free trial period and not particularly

breach of privacy. The data itself is also not to be considered as

privacy sensitive. In a balanced assessment, IMY believes that the company has shown

decisive legitimate reasons outweighing the appellant's interest in that his

card details can be reused to register new free trials on

the company's services and that his personal data shall not be processed.

IMY considers, against the background of the reasons put forward by the company, that the company has shown

decisive justified reasons that outweigh the appellant's interests, freedoms and

rights. The company has thus been justified in continuing to process the data after

the appellant has objected to the treatment and the appellant has therefore not been entitled to

deletion according to Article 17.1 c of the data protection regulation.

Has the company handled the complainant's requests in a formally correct manner according to

data protection regulation?

According to Article 12.1 of the Data Protection Regulation, the personal data controller must take

appropriate measures to provide to the data subject all communications according to

article 17 and 21 which refers to treatment in a concise, clear and clear, comprehensible and easy way

accessible form, using plain language, According to Article 12.3

data protection regulation, the personal data controller shall on request without unnecessary

delay and in any case no later than one month after receiving the request

provide the registrant with information about the measures taken pursuant to Article

17 and 21. According to Article 12.4, the personal data controller shall, if he does not take

measures at the request of the data subject, without delay and no later than one month after that

having received the request, inform the data subject of the reason for not taking action

taken and on the possibility of submitting a complaint to a regulatory authority and

request legal review. According to recital 59 of the data protection regulation should

obliged to respond to data subjects' requests and provide a justification, if they do not

intends to fulfill such requests.

In the case, only the company's actions during the time that

the data protection regulation has been applicable, i.e. since 25 May 2018. Vid

the assessment of whether the company fulfilled its information obligations towards

however, the appellant through his answer on 8 June 2018 must the answers that the company previously

submitted to the appellant is considered in favor of the company.

The company has brought forward, among other things, that the reason why the company in its response to the complainant

not informed about their legal basis for the processing, their balancing of interests or

the possibility of complaining to regulatory authorities was due to the complainant not being mentioned

personal data or the data protection regulation in their communication with the company and that

the complainant shortly before received information about this through the company's privacy policy

which came into force on 25 May 2018. However, IMY notes that the complainant expressly

stated that it concerned credit card information and for what purposes he meant that

the data may be processed, which can hardly be understood as anything other than as

personal data and references to the data protection regulations. As IMY stated above

and the company also stated itself, the appellant's request must also be understood as one

objection according to article 21, which has thus meant an obligation for the company to

notify the complainant of an individualized decision according to the data protection regulation.

Since the company's decision was negative, the company's response according to reason 59 would have been justified

and according to Article 12.4 contained the reason for this and complaint reference, which it did not

did. What the company stated that information about this appeared from the company's privacy policy is not enough. This is because it was an individualized one decision and the individual cannot be expected to take part in such a policy in its entirety in order to draw conclusions about the type of decision the company thus made, especially when the company neither indicated the legal basis on which the processing was based nor that the complainant's objection had been rejected.

Against this background, IMY finds that the company's response of 8 June 2018 was not sufficiently justified according to Article 12.4 because the company does not in a clear and unambiguous way has given an account of which data is processed, that the data is processed with the support of a legitimate interest and what the legitimate interest is and that the answer did not contain information about the possibility of submitting a complaint to the supervisory authority and request legal review. Spotify has thereby processed personal data in violation of Article 12.4 of the Data Protection Regulation.

Choice of intervention

From article 58.2 i and article 83.2 of the data protection regulation, it appears that IMY has power to impose administrative penalty charges in accordance with Article 83.

Depending on the circumstances of the individual case, administrative penalty fees are imposed in addition to or instead of the other measures referred to in article 58.2, such as injunctions and prohibitions. Furthermore, it is clear from article 83.2 which factors to be taken into account when deciding whether administrative penalty charges are to be imposed and when determining the size of the fee. If it is a minor violation receives IMY as set out in recital 148 in lieu of imposing a penalty charge issue a reprimand according to article 58.2 b. Consideration must be given to aggravating circumstances and mitigating circumstances of the case, such as the nature of the violation, degree of severity and duration as well as previous violations of relevance.

In its defense, the company has essentially stated that it is a one-off event

and that the company handles a large amount of customer service matters. Furthermore, since it has

happened the company's customer service advisers underwent further training in how they should

answer users in a clear and unambiguous way, which questions should be considered as

requests according to the data protection regulation and which questions should be forwarded

to the company's data protection team and data protection representative.

In an overall assessment of the circumstances, IMY finds that it is a question of a

such minor infringement in the sense referred to in recital 148 and that Spotify AB

therefore, a reprimand must be given in accordance with Article 58.2 b of the Data Protection Regulation for it

found the violation.

The case is closed.

This decision has been taken by the head of unit Catharina Fernquist after a presentation by

the lawyer Olle Pettersson.

Catharina Fernquist, 2021-03-24 (This is an electronic signature)

Copy to

The data protection officer

The Swedish Privacy Protection Authority

Diary number: DI-2020-10541

Date: 2021-03-24

How to appeal

If you want to appeal the decision, you must write to the Swedish Privacy Agency. Enter in

the letter which decision you are appealing and the change you are requesting. The appeal shall

have been received by the Privacy Protection Authority no later than three weeks from the day you received it part of the decision. If the appeal has been received in time, send
The Privacy Protection Authority forwards it to the Administrative Court in Stockholm examination.

You can e-mail the appeal to the Privacy Protection Authority if it does not contain any privacy-sensitive personal data or information that may be covered by secrecy. The authority's contact details appear on the first page of the decision.