Spotify AB

Org.nr: 556703-7485

Regeringsgatan 19

111 53 Stockholm

Record number:

DI-2020-10541

Date:

2021-03-24

Decision after supervision according to

the Data Protection Ordinance - Spotify AB

The decision of the Integrity Protection Authority

The 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 reply of 8 June

2018 on the complainant's objection to the consideration of 24 May 2018 according to

Article 21 has not clearly stated the information

processed, that the data are processed on the basis 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 Privacy Protection Authority gives Spotify AB a reprimand in accordance with Article 58 (2) b

the Data Protection Regulation.

Report on the supervisory matter

The Privacy Protection Authority (IMY) has initiated supervision regarding Spotify AB (Spotify)

or the company) in connection with a complaint. The complaint has been submitted to IMY, i

as the supervisory authority responsible in accordance with Article 56 of the Data Protection Regulation.

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

lodged its complaint (Denmark) in accordance with the provisions of the Regulation on cooperation

in cross-border treatment.

Postal 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 complainant has previously had one account and one

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

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

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

questions this, as the complainant's son has been refused registration for one

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

the card has already been used.

Spotify AB has mainly stated the following.

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the

natural persons with regard to the processing of personal data and on the free movement of such data and on

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

The complainant has requested deletion of his credit or debit card details. Spotify however, does not process card details when a user pays via PayPal, such as the complainant made, but instead deals with unique identifiers for the debit cards or "Instrument" ("unique payment instrument identifier") used by a customer at registration of free trial periods. The legal basis for the treatment is legitimate interests. That the complainant wrote that he withdraws his consent may be interpreted as an objection to the treatment. The continued treatment is not subject to the right to delete because Spotify has a strong, legitimate interest in continuing treatment which outweighs the complainant's rights and freedoms.

To sign up for a free trial period, potential customers must provide Spotify debit card information that will be used for billing when the free trial period has expired. To counteract the abuse of those free trial periods that the company offers use the company unique payment instrument identifier. This means that the same payment instrument can not used several times. Without this feature, it would be easy for a customer to launch new free Spotify accounts for additional trial periods each time their free trial period expires, by varying information such as e-mail address, and thus fraudulently utilizing Spotify. The unique payment instrument identifier is one alphanumeric chain generated by Spotify's payment processor PayPal. The allows the unique identification of credit cards, but it does not contain the credit card number or other card details. Spotify can not through the payment instrument identifier gain access to payment card details via

reverse engineering. This process is compatible with PCI

DSS2.

The processing is necessary for Spotify to be able to counter fraud. This is both

a legitimate interest in Spotify and the company's broad customer base, as 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 information since

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

the complainant's original request of 6 December 2017 and 8 June 2018 on

the complainant's latest request of 24 May 2018 and thus within the deadline in

the Data Protection Regulation. Regarding the complainant's letter of 15 March 2018

the company did not interpret it as a request for deletion under the Data Protection Regulation;

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

the complainant that the company does not store his debit card information and that the company does not

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

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

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

due to his objection, Spotify considers that the company responded to the complainant's

ask by explaining that it does not store any card information but only uses one

algorithm to see if a credit card has been used to take advantage of a Spotify offer

earlier. If the company had 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

customer service advisers communicate with users the company always tries to

provide the information that users request 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 the security of the use of credit and debit cards.

for users and also by someone unfamiliar with the provisions of

the Data Protection Regulation would understand. Because the complainant neither mentioned

regulation or asked for the legal basis for the processing went the company

does not go into legal details in its response such as the company's balancing of interests. In addition, had

the company in its privacy policy communicated to its users that it on request

is happy to provide more information about the balance of interests that the company has made

to rely on a legitimate interest as a legal basis and informed of the possibility

to lodge complaints with the supervisory authorities. Furthermore, it should be taken into account that the case

began more than five months before the entry into force of the Data Protection Regulation and that

the only correspondence that took place in the time after was the company's response two weeks

then. Since then, the company's customer service advisor has undergone additional training

in how to answer users in a clear and unambiguous way, what questions to consider

as inquiries in accordance with the Data Protection Regulation and the issues to be addressed

forwarded to the company's data protection team and data protection representative. Finally, it should

It is taken into account that the company receives more than 11,000 customer service cases daily. Although the company

customer service receive continuous training in data protection can be the human factor sometimes

lead to a case being answered as a customer service case instead of a response to one

request under the Data Protection Regulation referred to in Article 12 (4), in particular when

the user does not mention personal data or the data protection regulation in his

communication with the company.

The processing has taken place through correspondence. Given that it applies
cross-border treatment, IMY has used the mechanisms of cooperation
and uniformity contained in Chapter VII of the Data Protection Regulation. Affected
regulators have been the data protection authorities of Portugal, Belgium, Cyprus,
Austria, France, Germany, Slovakia, Italy, Spain, Denmark, Norway and
Finland.

Justification of decision

The Integrity Protection Authority's assessment

Has the company had the right to continue processing the complainant's information after that
the complainant objected to the treatment?

According to Article 17 (1) (c) of the Data Protection Regulation, the data subject shall have the right to do so
personal data controllers without undue delay have their personal data deleted and
the person responsible for personal data shall be obliged to delete without undue delay
personal data of the data subject objects to the processing in accordance with Article
21.1 and there are no justified reasons for the treatment which weighs heavier. According to the article
21.1, the data subject, for reasons relating to his or her specific
situation, have the right to object at any time to the treatment of
personal data relating to him or her based on Article 6 (1) (f)
the person responsible for personal data may no longer process the personal data unless he or she does not
can demonstrate decisive legitimate reasons for the treatment that outweigh it
registered interests, rights and freedoms.

The complainant's letter of 24 May 2018 may be understood as an objection to
treatment under Article 21 (1), for reasons relating to his specific situation in
in such a way that it means that the card number cannot be reused to register new ones
free trial periods on the company's services. Because the request had not been processed
before the data protection ordinance began to be applied on 25 may 2018, the company's must

the company has demonstrated decisive legitimate reasons for the treatment that outweigh

the interests, rights and freedoms of the data subject.

In order for treatment to be able to rely on Article 6 (1) (f), all three conditions must be met

provided therein are fulfilled, namely, first, that it

personal data controller or third party has a legitimate interest (legitimate interest),

secondly, that the treatment is necessary for purposes relating to the justifiable

interest (necessary) and thirdly that not the interests of the data subject or

fundamental rights and freedoms outweigh and require protection of

personal data (balancing of interests).

The company has stated, among other things, that the company's legitimate interest in the treatment is

to counter fraud regarding free trial periods. In recital 47

The Data Protection Regulation states that such processing of personal data is

absolutely necessary to prevent fraud constitutes a legitimate interest of the person concerned

personal data controller. IMY thus considers that the company has a legitimate interest.

Furthermore, the IMY considers that the treatment is absolutely necessary for purposes relating to it

legitimate interest. The investigation shows that the information has been minimized

to the extent possible for the company to be able to achieve the purpose that pertains to it

legitimate interest.

In the balance of interests to be made between the company's legitimate interest and

the complainant's interests, rights and freedoms, IMY states that the company's justified

interest weighs heavily. The treatment appears to be something that the complainant reasonably can

expect when registering a free trial period and not specifically

invasion of privacy. The data itself is also not to be regarded as

privacy sensitive. In a weighted assessment, IMY considers that the company has shown

decisive legitimate reasons which outweigh the appellant's interest in his

card data can be reused to register new free trial periods of

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

In the light of the reasons put forward by the company, IMY considers that the company has shown

crucial legitimate reasons which outweigh the interests, freedoms and freedoms of the appellant

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

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

deletion in accordance with Article 17 (1) (c) of the Data Protection Regulation.

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

the Data Protection Regulation?

According to Article 12 (1) of the Data Protection Regulation, the controller shall take

appropriate measures to provide the data subject with all communications under

Articles 17 and 21 which relate to treatment in a concise, clear and distinct, comprehensible and easy

available form, using clear language, In accordance with Article 12 (3)

data protection regulation, the data controller shall, upon request, without undue need

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

provide the data subject with information on the measures taken pursuant to Article

17 and 21. According to Article 12 (4), the data controller shall, if he does not take action

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

have received the request inform the data subject of the reason why action is not

taken and on the possibility of lodging a complaint with a supervisory authority and

request legal action. According to recital 59 of the Data Protection Regulation

data controllers without undue delay and within one month at the latest

obliged to respond to the data subjects' requests and provide a justification, if they do not
intends to fulfill such wishes.

In the case, the company's actions must only be assessed during the period that
the Data Protection Regulation has been applicable, ie since 25 May 2018. At
the assessment of whether the company has fulfilled its information obligations towards
the complainant through its response on June 8, 2018, however, the responses provided by the company earlier
submitted to the complainant is taken into account for the benefit of the company.

The company has, among other things, stated the reason why the company in its response to the complainant
not informed of its legal basis for the treatment, its balancing of interests or
the possibility of complaining to regulators is due to the fact that the complainant did not mention
personal data or the Data Protection Ordinance in its 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. IMY notes, however, that the complainant expressly
stated that it concerns credit card information and for what purposes he intended to
the data may be processed, which can hardly be understood as anything other than that
personal data and references to the data protection rules. As IMY stated above
and the company also stated itself, the complainant's request must also be perceived as one
objection under Article 21, which has thus entailed an obligation for the company to:
notify a decision individualized for the complainant in accordance with the Data Protection Regulation.
Since the company's decision was negative, the company's response under recital 59 would have been justified
and according to Article 12 (4) contained the reason for this and referral of complaints, 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 is an individualized

decision and the individual can not be expected to take part in such a policy in its entirety to

draw conclusions about the type of decision the company has made, especially when the company

neither stated the legal basis on which the proceedings were based nor that of the appellant

objection had been rejected.

Against this background, IMY finds that the company's response of 8 June 2018 has not been

sufficiently justified in accordance with Article 12 (4) as the company does not clearly and unequivocally

has reported which data is processed, that the data is processed on the basis of

a legitimate interest and what the legitimate interest is and that the answer did not contain

information on the possibility of submitting a complaint to the supervisory authority and

request legal action. Spotify has thereby processed personal data in violation of

Article 12 (4) of the Data Protection Regulation.

Choice of intervention

Article 58 (2) (i) and Article 83 (2) of the Data Protection Regulation state that the 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 in place of the other measures referred to in Article

58.2, such as injunctions and prohibitions. Furthermore, Article 83 (2) states which

factors to be taken into account when deciding on administrative penalty fees shall be imposed

and in determining the amount of the fee. In the case of a minor infringement

receive IMY as set out in recital 148 instead of imposing a penalty fee

issue a reprimand in accordance with Article 58 (2) (b). Account shall be taken of aggravating and

mitigating circumstances in the case, such as the nature of the infringement, the degree of difficulty

and duration as well as previous violations of relevance.

In its defense, the company has mainly stated that this is a one-off event

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

occurred the company's customer service advisors have undergone further training in how to

answer users in a clear and unambiguous way, what questions to consider

inquiries in accordance with the Data Protection Ordinance and which issues are to be forwarded

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

The IMY finds in an overall assessment of the circumstances that it is a question of one

such minor infringement within the meaning of recital 148 and that Spotify AB

therefore, a reprimand must be granted in accordance with Article 58 (2) (b) of the Data Protection Regulation for it

found the infringement.

The case is closed.

This decision has been made by Catharina Fernquist, Head of Unit, after a presentation by

lawyer Olle Pettersson.

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

Copy to

The Data Protection Officer

Integrity Protection Authority

How to appeal

If you want to appeal the decision, you must write to the Privacy Protection Authority. Enter i

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

part of the decision. If the appeal has been received in time, send

The Integrity 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 data that may be covered by

secrecy. The authority's contact information can be found on the first page of the decision.