Swedish Authority for Privacy Protection

Spotify AB
Org. no:556703-7485
Regeringsgatan 19
111 53 Stockholm

Our ref.:
DI-2020-10541, IMI no. 75661

Date:
2021-03-24

Supervision under the General Data Protection Regulation – Spotify AB

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

The Swedish Authority for Privacy Protection (IMY) finds that Spotify AB has processed personal data in violation of

- Article 12(4) of the General Data Protection Regulation (GDPR)[1] by in its reply of 8 June 2018 to the complainant's objection to the processing pursuant to Article 21 of 24 May 2018 having not clearly stated what personal data is being processed, that the data is processed on the basis of a legitimate interest and what the legitimate interest is and that the answer has not contained information about the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

The Swedish Authority for Privacy Protection (IMY) issues Spotify AB a reprimand in accordance with Article 58(2)(b) of the GDPR.

Report on the supervisory matter

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

The *complaint* is essentially the following. The complaint has previously had an account and a payment subscription to the company's music service. The complainant has several times requested that the company erase his card details. According to the company, the complainant has registered via PayPal and the company therefore does not process the complainant's card details. The complainant questions this because the complainant's son has been refused to register for a free trial period where the

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

[1] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with respect to the processing of personal data and on the free flow of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

complainant's card information has been used, on the grounds that the card has already been used.

Spotify AB has mainly stated the following.

The complainant has requested deletion of his credit or debit card information. However, Spotify does not process card data when a user pays via PayPal, such as the complainant, but instead treats unique identifiers for the payment cards or "instruments" ("unique payment instrument identifiers") used by a customer when registering free trial periods. The legal basis for the processing is legitimate interests. That the complainant has written that he withdraws his consent may be interpreted as an objection to the processing. The continued processing is not subject to the right to erasure because Spotify has a strong, legitimate interest in continuing the processing that outweighs the rights and freedoms of the complainant.

To register for a free trial, potential customers must provide Spotify debit card details that will be used for invoicing once the free trial has expired. To counter the abuse of the free trials offered by the company, the company uses unique payment instrument identifiers. This means that the same payment instruments cannot be 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 expires, by varying tasks such as email address, and thus fraudulently exploiting Spotify. The unique payment instrument identifier is an alphanumeric chain generated by Spotify payment processor PayPal. It allows for the unique identification of credit cards, but it does not contain the credit card number or other card details. Spotify cannot, through the payment instrument identifier, access to debit card information via reverse engineering. This process is compatible with PCI DSS[2].

The processing is necessary for Spotify in order to counteract fraud. This is both a legitimate interest in Spotify and the company's broad customer base, as the company could not continue to offer free trials of the company's service if fraud could not be counteracted in this way. It is also in the public's legitimate interest.

Spotify has responded to the complainant's request but has not deleted the data because the right to erasure is not applicable. The company responded on 7 December 2017 to the complainant's original request of 6 December 2017 and 8 June 2018 to the complainant's most recent request of 24 May 2018 and thus within the deadline of the GDPR. Regarding the complainant's letter of 15 March 2018, the company did not interpret it as a request for deletion under the GDPR, but responded to the letter on 4 May 2018. In several of these answers, the company has informed the complainants that the Company does not store his debit card information and that the company could not erase the payment instrument reference that identifies that his card has already been used to access one of the company's offers or services.

Regarding the information provided to the complainant on 8 June 2018 due to his objection, Spotify believes that the company responded to the complainant's question by explaining that it does not store any card information but only uses an algorithm to see if a credit card has been used to access a Spotify offer earlier. If the company had had reason to believe that the complainant wanted more details about these categories of personal data, the company would have provided it. When the company's customer service advisors communicate with users, the company always

[2]PCI DSS stands for Payment Card Industry Data Security Standard and is a widely accepted set of guidelines and procedures aimed at optimising security around the use of credit and debit cards.

tries to provide the information that users ask for in a format that is relevant to the users and which also someone who does not know the provisions of the GDPR would understand. Since the complainant neither mentioned the regulation nor asked for the legal basis for the processing, the company did not address legal details in its response such as the company's balance of interests. In addition, in its privacy policy, the company had communicated to its users that it would like to provide more information on the weighing of interests that the Company has made to rely on legitimate interest as a legal basis and informed of the possibility of filing a complaint with the supervisory authorities. It should also be taken into account that the matter was started more than five months before the GDPR came into force and that the only correspondence that took place in the time after was the company's response two weeks thereafter. Since then, the company's customer service advisors have undergone further training on how to answer users in a clear and clear manner, which questions should be regarded as inquiries under the GDPR and what questions should be forwarded to the company's data protection team and data protection officer. Finally, it must be taken into account that the company receives over 11,000 customer service cases daily. Although the company's customer service receives continuous data protection training, the human factor can sometimes lead to a matter being answered as a customer service case instead of a response to a request under the GDPR referred to in Article 12(4), especially when the user does not mention personal data or the GDPR in his communication with the company.

The investigation has been carried out in written form. In the light of cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Portugal, Belgium, Cyprus, Austria, France, Germany, Slovakia, Italy, Spain, Denmark, Norway and Finland.

Justification of the decision

The assessment of the Authority for Privacy Protection (IMY)

Has the company had the right to continue processing the complainant's data after the complainant objected to the processing?
According to Article 17(1)(c), the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay when the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing. According to Article 21(1) the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on Article 6(1)(f). The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject.

The complainant's email to the company of 24 May 2018 must be understood as an objection to the processing pursuant to Article 21(1), for reasons related to his specific situation, being that the card number cannot be reused to register new free trial periods on the company's services. Since the objection had not been handled before the introduction of the GDPR on 25 May 2018, the company's processing of requests must be assessed in accordance with the GDPR, i.e. whether the company has

demonstrated compelling legitimate grounds for processing that outweighs the interests, rights and freedoms of the data subject.

In order for processing to be based on Article 6(1)(f), all three conditions provided therein must be fulfilled, namely, firstly, that the controller or third party has a legitimate interest (*legitimate interest*), secondly that the processing is necessary for purposes of legitimate interest (*necessary*) and third that the interests or fundamental rights and freedoms of the data subject do not weigh heavier and require the protection of personal data (*balance of interest*).

Among other things, the company has stated that the company's *legitimate interest* with the processing is to counteract fraud regarding free trial periods. Recital 47 of the GDPR states that processing of personal data that is absolutely necessary to prevent fraud constitutes a *legitimate interest in* the controller concerned. IMY therefore considers that the company has a legitimate interest.

Furthermore, IMY believes that processing is absolutely *necessary* for purposes relating to legitimate interest. The investigation shows that the data has been minimised insofar as it is possible for the company to achieve the purpose of the legitimate interest.

In the *weighing of interests* to be made between the Company's legitimate interest and the interests, rights and freedoms of the complainant, IMY notes that *the company's legitimate interest* weighs heavily. The processing appears as something that the complainant can reasonably expect when registering a free trial and not particularly privacy invasive. The personal data in question can neither be considered as sensitive from a privacy perspective. In a summarized assessment, IMY finds that the company has demonstrated compelling legitimate grounds that outweigh *the complainant's interest in the* reuse of his card information to register new free trial periods on the company's services and that his personal data shall not be processed.

In light of the reasons the company has presented, IMY finds that the company has demonstrated compelling legitimate grounds that outweigh the complainant's interests, freedoms and rights. The Company has thus had the right to continue processing the data after the complaint has objected to the processing and the complaint has therefore not been entitled to erasure under Article 17(1)(c) GDPR.

Has the company handled the complainant's requests in a formally correct manner under the GDPR?

According to Article 12(1) of the GDPR, the controller shall take appropriate measures to provide any communication under Article 17 and 21 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Pursuant to Article 12(3) the controller shall provide information on action taken on a request under Article 17 and 21 to the data subject without undue delay and in any event within one month of receipt of the request. If the controller does not take action on the request of the data subject the controller shall pursuant to According to Article 12(4) inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy. According to Recital 59 of the GDPR, the controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

In the present case, the legality of the Spotify's actions shall only be assessed during the period when the GDPR has been applicable, i.e. since 25 May 2018. However, when assessing whether the company has fulfilled its information obligations to the complainant through its reply on 8 June 2018, the answers that the company previously submitted to the complainant shall be taken into account for the company's benefit.

Spotify has stated, among other things, that the reason why the company in its reply to the complainant has not informed of its legal basis for the processing, its balancing of interests or the possibility to complain to supervisory authorities was due to the fact that the complainant did not mention personal data or the GDPR in his communications with the company and that the complainant shortly before received information about this through the company's privacy policy that came into force on 25 May 2018. However, IMY notes that the complainant expressly stated that his concern was about credit card information and for what purposes he meant that the data may be processed, which can hardly be understood as other than personal data and references to data protection rules. As stated above and as the company itself has found, the complainant's request must also be perceived as an objection pursuant to Article 21, which has thus entailed an obligation for the company to take an individualised decision to complainant pursuant to the GDPR. Since the company's decision was negative, the company should have informed of the reasons for its decision in accordance with Article 12(4) and included information about the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy, which it did not. What the company has stated that information about this has been disclosed by the company's privacy policy is not sufficient. This because the matter concerns an individualised decision and a data subject cannot be expected to review such a policy in its entirety to deduce what type of decision the company has made, especially when the company's response neither provided the legal basis for which the processing was based or information that an objection pursuant to the GDPR from the complainant had been rejected.

Against this background, IMY finds that the company's response of 8 June 2018 has not been sufficiently justified pursuant to Article 12(4) because the company has not clearly stated what personal data is being processed, that the data is processed on the basis of a legitimate interest and what the legitimate interest is and that the answer has not contained information about the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy. Spotify has thus processed personal data in violation of Article 12(4) GDPR.

Choice of corrective measure

Articles 58(2) and 83(2) of the GDPR states that IMY has the authority to impose administrative fines in accordance with Article 83. Depending on the circumstances of the individual case, administrative fines shall be imposed in addition to or instead of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) lists which factors should be taken into account in deciding whether to impose an administrative fine and on the amount of the fine. If it is a minor infringement, IMY may, as stated in recital 148 instead of impose an administrative fine, issue a reprimand pursuant to Article 58(2)(b). Consideration shall be taken to aggravating and mitigating circumstances in the case, such as the nature of the infringement, severity and duration as well as previous relevant infringements.

In its defence, the company has mainly stated that it is a one-time occurrence and that the company handles a large number of customer service matters. Furthermore, since the company's customer service advisors have undergone further training on how to answer users in a clear and clear manner, which questions should be considered as inquiries under the GDPR and what questions should be forwarded to the company's data protection team and data protection officer.

In an overall assessment of the circumstances, IMY finds that the stated infringements are minor violations in the sense referred to in recital 148 and that Spotify AB therefore should be issued a reprimand in accordance with Article 58(2) of the GDPR for the stated infringements.

This decision has been made by Head of Unit Catharina Fernquist after presentation by legal advisor Olle Pettersson.

Notice. This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2021-03-24, no. DI-2020-10541. Only the Swedish version of the decision is deemed authentic.