Swedish Authority for Privacy Protection

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision 2023-05-22, no. IMY-2022-9109. Only the Swedish version of the decision is deemed authentic.

Ref no:
IMY-2022-9109

Date of decision:
2023-05-22

Decision pursuant to Article 60 under the General Data Protection Regulation – MAG Interactive AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection finds that MAG Interactive AB (556804-3524) in handling the request for erasure that the complainant made on 31 January 2021 has processed personal data in violation of:

- article 12.6 of the General Data Protection Regulation (GDPR)[1] by requesting information in the form of usernames of three friends and three opponents in the game QuizDuel when this was not necessary to confirm the complainant's identity and
- article 12.2 of the GDPR by, after the complainant requested erasure by email, also requiring the complainant to log in to the game to send the request from within the game, which has not facilitated the complainant's exercise of the complainant´s right to erasure.

The Swedish Authority for Privacy Protection issues a reprimand to MAG Interactive AB pursuant to Article 58(2)(b) of the GDPR for infringement of Articles 12(2) and 12(6) of the GDPR.

Presentation of the supervisory case

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding MAG Interactive AB (the company) due to a complaint, essentially to investigate if MAG Interactive AB has received and handled the complainant's request for erasure correctly, i.e. if the company had reasonable grounds to doubt the identity of the complainant and in such case if the information requested from the complainant was necessary to confirm the identity of the complainant and whether the company has facilitated the exercise of the complainants´ rights to a sufficient extent (Articles 11, 12 and 17 of the GDPR). The complaint has been submitted to IMY, as the lead 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

[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

their complaint (France) in accordance with the provisions of the GDPR on cooperation in cross-border processing.

The case has been handled through written procedure. In the light of the complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The concerned supervisory authorities concerned have been the data protection authorities in Denmark, France, Ireland, Norway, Poland, Germany and Austria.

The complaint
In the complaint the following is mainly stated.

On 31 January 2021, the complainant requested erasure of their personal data in the game QuizDuel, a game that the complainant used through their Facebook account. MAG Interactive AB requested further information from the complainant for the purposes of identification even though the complainant in their request for erasure, stated their Facebook ID and email addresses. To the complaint the complainant has attached the correspondence between the complainant and the company of what among other things the following appears. On 28 February 2021, the company replied that it is not in a position to locate, using the complainant's Facebook ID, the complainant's account and that the complainant needs to open any of the MAG Interactive-games to make a request. The complainant replied that they no longer have an MAG Interactive account. On 11 March 2021, the company requested the following information from the complainant in the purpose of restoring the complainant's account and thus enabling the complainant to request erasure of their personal data: username, name of three friends, names of three opponents and an email address to which they want to link the account.

What the company has stated
The company has mainly stated the following in its statements from the 4 and 7 of November 2022.

Description of the course of events relating to the handling of the complainant's request for erasure

On 31 January 2021, the complainant contacted one of the company's support email addresses and provided a Facebook ID and three email addresses and requested to be erased. By this time, given the information the support received, the company did not receive any hits at a direct search in the company's system, neither on the Facebook ID nor on any of the specified email addresses. The company's support responded on 1 February 2021 with instructions for how the complainant can request erasure from the game. The complainant contacted the company again on 8 February 2021 and said they don't have the game left but want to get rid of their data. On 9 February 2021 the company's support replied that the easiest way is to download the game again and request erasure from within the game. On 12 February 2021, the complainant replied and said they wanted to know what information the company had about them. From this time on, the case was handled by the company as a request for access.

On 13 February 2021, the company's support replied that the complainant may request access from within the game. The complainant contacted the company again on 20 February 2021 and had problems with using their Facebook account. The complainant asked again if the company could find their account with their Facebook

ID. On 23 February 2021, the support team replied that they did not find any account with the Facebook ID provided by the complainant but that they should be able to start any of the company's games and request the personal data from within a game.

On 27 February 2021, the complainant asked whether the company had actually tried searching on their Facebook ID. The support responded again on 28 February 2021 that they cannot find their account on the Facebook ID they specified but that they should be able to start any of their games and request access from within the game. On 4 March 2021, the complainant replied that they played 'QuizDuel' on Facebook and does not have an account with MAG Interactive. Therefore, they cannot request access from there. This was probably a misunderstanding as the game never existed on Facebook but they may have logged in via a Facebook button originally which was possible several years ago. It was the first time that the complainant mentioned the game in question, which made it much easier to look for their data.

On 11 March 2021, the support replied that they do not find the complainant's account via their Facebook ID but that they should try to help them access their account so that they can request access or delete their account. The support had then likely managed to locate an account linked to one of the complainant's specified email addresses using the information about the game. The support then sent the standard questions the company asks when the company helps users access their account if they have forgotten their user details. The complainant never replied to that email and when sufficient time had passed, the company closed the case.

On 30 October 2022, after the company´s CTO had received the case, the CTO located an account that could be linked to the complainant and emailed the complainant to obtain confirmation that the account should be erased. On 6 November 2022, the complainant replied, confirming that they own the account and that the account should be erased. On 7 November 2022, the complainant's account was erased and the complainant was informed thereof.

Processing of the complainant's personal data by the company at the time of the complainant's request

At the time of the complainant's request for erasure, it processed an email address associated with the complainant and probably advertisingId/vendorId from their telephone, the complainant's username and password. Otherwise, the company did not process any other of the complainant's personal data because any chat history and IP number has long been deleted due to the company's retention policy.

Why the company claims to have had reasonable grounds to doubt the identity of the complainant

In their request for erasure, the complainant indicated a Facebook ID and three email addresses and wrote that they had used one of the company's apps on Facebook.

The company's games are played not on Facebook but on mobile phones and they did not provide any surrounding information such as username, which game it was or even that it was a game. The game that the complainant, according to later reportedly, had played is so old that the company neither got any hits on the other email addresses. Moreover, since the game which the complainant's user account is tied to since long is closed, it makes it difficult to find it only with an email address. Email addresses are public and an indication of an email address is therefore not proof of ownership. The

email address from which the request came was also not linked to any account with the company or to the Facebook ID provided. As regards the other two e-mail addresses, there was no evidence that these were the complainant's email addresses.

The Facebook ID provided by the complainant is not registered with the company. Since many years, Facebook has stopped using global user numbers for privacy reasons. In the service that the company suspended many years ago, where it was possible to log in via a Facebook account, the company does not see the same number as the complainant indicates. The customer number the company received from Facebook is only linked to the company and cannot be linked to a person's Facebook account.

Given the knowledge of which game it concerns that the company eventually got, it would have been possible to find the account to which one email address was linked. The company could then have sent an email to that email address in order to confirm the complainant's identity. However, it had not played any role in this case when on 13 February 2021 the case was changed to a request for access.

How the complainant should proceed to request erasure and subsequent access

The support initially suggested that the complainant should request erasure directly from the game as it is the simplest and safest way. Normally, users still have the game on the phone. In addition, the company's games at a reinstallation help the user get back to the correct account. Therefore, when support has difficulty finding an account with the user's details, it is reasonable that they suggest a reinstallation to get to the correct account. Support can also delete information directly if ownership of the information can be substantiated. In the present case, the case turned to a request for access and then the company normally wants the user to be logged in to its account. The company has stated that just as for the request for erasure, proof of ownership of the account is required to request access, for reasons of privacy and in accordance with the GDPR. As user data may contain chat logs, the handling of the access request is a little more stringent than when handling a request for erasure of user data. The company therefore requires that the request be made from within the player's account.

Information requested for the purpose of verifying the identity

The game that the complainant had played was a game with user accounts. In games with user accounts, there are often chats for players to be able to talk to each other. For privacy reasons, it is important that anyone can not read someone else's chats. The accounts are therefore password protected. Users can enter an email address for password reset, but not all users do, or they have changed their email address.

One question all online services struggle with is how to handle cases where users forgot their login details and it is not possible to reset the account via email. Some use security questions, where users are allowed to fill in the name of their first pet or similar. In the company's case, it is a little more complicated because, as the company does not want to ask users for more information than absolutely necessary and the game concerned in the present case has a user base built since 2012 with 100 million users who have not entered such information. Once the user has forgotten the login details and the account cannot be restored via email, the company resolves this by using information on the phone and the operating system to help users back to the

account, which is why support sometimes asks users to install the game, which also the support has done in this case.

When it doesn‘t work, or as in this case, when the user doesn’t want to, the support ask as a last resort for information that the user should know and that should be easy for a user to remember but that is difficult for others to know about. This information is requested in order for the company to ensure that it is the account holder that they give access to the account. The information requested by support in such cases is the following:

- User name of the data subject. Information that is assumed to be easy for most people to provide. However, it is also information that is relatively easy for others to find out.

- Username of three of the registered friends in the game. Most people who play this game have some friends they've been playing with for years. This information should also be easy to answer.

- Username of three of the registered opponents in the game. This information is often a little harder to provide but for users who mostly play against random players and do not add friends, it is necessary information.

The support also asked for the email address the user wanted to link the account to. This is in order for the complainant to be able to log in and request their user details from within the game.

The data shall normally be provided by email in the ongoing support dialogue. It is not a requirement to be right on all questions, but an assessment is made based on how right/wrong the answer is. Nor does the Company ask for personally identifiable information, but only for usernames that are normally anonymous/pseudonymous and which are already in the company’s register. The only information that is personally identifiable information is the email address the user wants to link to the account. If the user can respond so well that the company determines that the user actually owns the account, the support will set the email address for recovery. The user can then set a new password and log in.

The company is continuously working on improving its support tools and will shortly release a new version where this particular scenario can be managed and which will make it easier for support to find users even with very limited information. Support is instructed to erase the user’s account immediately if the email address on the account matches the user’s email address and otherwise help the user erase the account through the game. In this case, the company can imagine a third solution, that the company email out a link to the linked account and that the user confirms erasure via the link to verify their identity. The company intends to add such possibility.

The complainant’s account has been deleted

The complainant’s request for erasure has now been met. The company has emailed the complainant on 30 October 2022 both at the email address they used in the support case and the email address they were found when searching. The company’s CTO asked the complainant to reply from that email address. A reply from the complainant was received on 6 November 2022 confirming that they own the account.

The CTO subsequently erased the complainant's account and informed the complainant accordingly.

Statement of reasons for the decision

Applicable provisions, etc.

Pursuant to Article 17(1), 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 where one of the grounds listed in the Article applies, for example where the data are no longer necessary for the purposes for which they have been collected or where consent for processing is withdrawn.

Article 11(1) states that where the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

According to Article 11(2), where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

Article 12(6) states that, without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

Article 12(2) requires the controller to facilitate the exercise of the data subject's rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

The European Data Protection Board's (EDPB) Guidelines 01/2022 on access[2] state, inter alia, the following:

> 53. The EDPB encourages controllers to provide the most appropriate and user-friendly communication channels, in line with Art. 12(2) and Art. 25 GDPR, to enable the data subject to make an effective request. Nevertheless, if a data subject makes a request using a communication channel provided by the controller, which is different from the one indicated as the preferable one, such request shall be, in general, considered effective and the controller should handle such a request accordingly (see the examples below). The controllers should undertake all reasonable efforts to make sure that the exercise of data subject rights is facilitated (for example, when a data subject sends an access request to an employee who is

[2] EDPB, Guidelines 01/2022 on data subject rigts – Right of access, version 2.0, adopted on 28 March 2023.

on leave, an automatic message informing the data subject about an alternative communication channel for this request could be a reasonable effort).

[…]

67. In cases where the controller requests or is provided by the data subject with additional information necessary to confirm the identity of the data subject, the controller shall, each time, assess what information will allow it to confirm the data subject's identity and possibly ask additional questions to the requesting person or request the data subject to present some additional identification elements, if it is proportionate (see section 3.3).

68. In order to allow the data subject to provide the additional information required to identify his or her data, the controller should inform the data subject of the nature of the additional information required to allow identification. Such additional information should not be more than the information initially needed for the authentication of the data subject. In general, the fact that the controller may request additional information to assess the data subject's identity cannot lead to excessive demands and to the collection of personal data which are not relevant or necessary to strengthen the link between the individual and the personal data requested.

[…]

70. As indicated above, if the controller has reasonable grounds for doubting the identity of the requesting person, it may request additional information to confirm the data subject's identity. However, the controller must at the same time ensure that it does not collect more personal data than is necessary to enable authentication of the requesting person. Therefore, the controller shall carry out a proportionality assessment, which must take into account the type of personal data being processed (e.g. special categories of data or not), the nature of the request, the context within which the request is being made, as well as any damage that could result from improper disclosure. When assessing proportionality, it should be remembered to avoid excessive data collection while ensuring an adequate level of processing security.

[…]

138. The use of self-service tools should never limit the scope of personal data received. If not possible to give all the information under Art. 15 through the self-service tool, the remaining information needs to be provided in a different manner. The controller may indeed encourage the data subject to use a self-service tool that the controller has set in place for handling access requests. However, it should be noted that the controller must also handle access requests that are not sent through the established channel of communication.

Assessment of IMY

On the basis of the complaint in question, IMY examined the company's conduct in this individual case.

Has the company been able to identify the complainant?

The company states that, on the basis of the information contained in the complainant's request for erasure on 31 January 2021, the company was not in a position to identify the data subject. According to the company´s statement, the information provided by the complainant in the request did not result in a direct finding in the company's system, neither on the Facebook ID nor on any of the email addresses provided by the complainant. The company further states that when they on 4 March 2021 received information on which game the complainant´s request concerned, they were able to find an account to which one of the complainant's e-mail addresses was linked to. In light of this, IMY notes that, at least on 4 March 2021, the company was able to link the complainant's request to a user account and that identification of the complainant was thus possible. IMY therefore considers that, in accordance with the provisions of Article 11(2) of the GDPR, the complainant provided such additional information which made identification possible. The company has thus not demonstrated that it was not in a position to identify the data subject and could therefore not refuse to comply with the data subject's request to exercise their rights under Article 12(2) of the GDPR.

Has the company acted in accordance with 12(6) of the GDPR when the company requested current information from the complainant?

Has the company had reasonable grounds to doubt the identity of the complainant

It is only where the controller has reasonable grounds to doubt the identity of the person making the request that additional information to confirm the identity may be requested. What constitutes "reasonable grounds" in Article 12(6) GDPR should be assessed on the basis of the circumstances of the individual case. The assessment of whether there are reasonable grounds to doubt the identity of the one making a request is normally made in the light of the information provided in connection with the request. This applies particularly in situations where the controller has no further knowledge of that person. However, the need for an individual assessment does not preclude the establishment of procedures for how the controller normally verify the identity of the data subject.

It appears from the annex to the complaint that the complainant provided the following information when requesting erasure on 31 January 2021: Facebook ID and three email addresses as well as one email address from which the request email was sent.

The company states that, at the time of the complainant's request for erasure, they processed an email address associated with the complainant and probably also the advertisingId/vendorId from the complainant's telephone, the complainant's username and password.

The company was given the opportunity to motivate the individual assessment made from the complainant's situation if the company considered that it had reasonable grounds to doubt the identity of the complainant when they made their request. The company stated mainly the following. The company's games are not played on Facebook but on mobile phones, so Facebook ID did not contribute to the verification of the complainant's identity. Email addresses are public and a statement of such is not a proof of ownership. The email address from which the request was made was also not linked to any account with the company or to the Facebook ID provided. The complainant did not provide any surrounding information such as user name, which game it concerns or even that it is a game. The game played by the complainant, according to later provided information, was so old that the company did not receive

any search findings on the other email addresses provided in the request. On 4 March 2021, on the basis of the information provided by the complainant on which game the request concerns, the company found a user account linked to one of the complainant's e-mail addresses.

In the light of the company´s submissions and the information provided by the complainant in their request for erasure, IMY finds that the company had reasonable grounds to have doubts concerning the identity of the complainant. In the assessment, IMY also takes into account the fact that the obligation to ensure the identity of the person making the request is also intended to protect data subjects against someone else making inaccurate requests in their name, which may lead to negative consequences for the data subjects.

Has the information requested by the complainant been necessary to confirm their identity?

Although the controller has reasonable grounds to doubt the identity of the data subject, the controller shall not collect more personal data than is necessary to enable the identification of the requesting data subject. The controller shall carry out a proportionality assessment and be able to justify the verification method used.

The company has stated that the request was changed to a request for access on 4 March 2021, and the company then required that the request be made from within the user's account. As user data may contain chat logs, the handling of the access request is a little more stringent than when handling a request for erasure of user data, the company has stated. As regards the necessity of the information the company has requested from the complainant in order to confirm their identity, the company has stated, mainly the following. Usernames are requested as the information is assumed to be easy for most people to answer. However, it is information that is relatively easy for others to find out. The usernames of three friends in the game are requested as most people who play this game have some friends they have been playing with for years. That information should therefore be easy to provide. The usernames of three opponents in the game are harder to provide but for people who mostly play against random players and do not add friends, it is necessary information to request. It is not a requirement that the person making the request gives right answers to all questions, but an assessment is made based on how right or wrong the answer is.

IMY notes that it appears from the material the company has submitted, consisting of the correspondence between the complainant and the company, that the complainant did not withdraw their request for erasure. Furthermore, it appears from the email correspondence, in particular the email sent by the MAG Support Team on 11 March 2021, that the data in question were requested by the company in order to enable the complainant to access the account for the purpose of requesting erasure. The company's claim that the complainant's request for erasure had been changed to a request for access, and that the requested information intended to identify the complainant only in the event of a request for access, can therefore be disregarded. The company has indeed requested further information from the complainant in order to confirm the complainant´s identity, however IMY considers that it appears that it is still a request for erasure that the complainant wants to be granted. It also appears that the company requested the information in connection with the complainant's request for erasure.

As regards the information requested by the company from the complainant, IMY states the following. It follows, inter alia, from the EDPB's guidelines on the right of access that the controller must take into account in the proportionality assessment the type of personal data processed (e.g. special categories of data or not), the nature of the request, the context in which the request is made and any harm that may arise as a result of improper disclosure. At the time of the complainant's request, the company processed only one email address associated with the complainant and the advertisingId/vendorId from their telephone, the complainant's username and password. In IMY's view, an erroneous erasure of that information would not have any significant disadvantages or consequences for the complainant. The requirements for identification could thus be set relatively low. Furthermore, it has been shown that correct answers to all the questions were not required and that the identity of the complainant was subsequently confirmed by a different method of identification which required considerably fewer data. Confirmation that it is the complainant's user account sent from the e-mail address linked to the user account was deemed sufficient to confirm the complainant's identity and to comply with the request on 7 November 2022.

IMY therefore considers that, taking into account the nature of the request, the type of personal data processed and the method of identification subsequently used, the data in the form of the usernames of three friends and three opponents cannot be considered necessary or proportionate to confirm the identity of the complainant in accordance with Article 12(6) of the GDPR.

Has the company facilitated the exercise of the right to erasure under Article 12(2) of the GDPR?

The next question is whether it has been compatible with Article 12(2) GDPR to require the complainant to log in their account and make their request from within the game.

In essence, the company stated the following. If the user can respond so well that the company determines that the user owns the account, the support will set the email address for recovery. The user can then set a new password and log in. Since, in the present case, the case had changed to a request for access, the company normally want the user to be logged in to their account in order to exercise their request.

As IMY noted in the section above, it appears from the material the company submitted that the complainant did not withdraw from their request for erasure and that the company requested the data in question in order to enable for the complainant to access the account in order to request erasure from within the game.

The EDPB's guidelines on access state, among other things, that the controller may encourage the data subject to use a self-service tool, but that the controller must also handle requests for access that are not sent through the established communication channel. By requiring the complainant, whose request for erasure has been received by the company, that, after answering questions intended to confirm their identity, they must log in to a game in order to send their request from within the game, the company has not made it easier for the complainant to exercise their right to erasure. IMY therefore considers that the company thereby acted in breach of Article 12(2) of the GDPR.

Has the complainant's request for erasure pursuant to Article 17 GDPR been complied with?

The complaint shows that the complainant requested erasure on 31 January 2021 and that it has not been satisfied at the time of the complaint. The company states that on 7 November 2022, following correspondence with the complainant on 30 October and 6 November 2022, the company erased the complainant's data and the complainant was informed thereof. Since the complainant's request for erasure has now been met, there is no reason to investigate the matter further in that part.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that 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) determines the factors to be taken into account when imposing administrative fines and when determining the amount of the fine. In the case of a minor infringement, IMY may, as stated in recital 148, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Account needs to be taken to the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement as well as past infringements of relevance.

IMY notes the following relevant facts. The current supervision covers MAG Interactive AB's handling of an individual complainant's request for erasure and the established infringements are relatively far back in time (2021). MAG Interactive AB has now also fully complied with the complainant's request for erasure. Against this background, IMY considers that it is a minor infringement within the meaning of recital 148 and that MAG Interactive AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

This decision has been taken by the specially appointed decision-maker, legal advisor [redacted], following a 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.