Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision.

CONTROLLER
Paradox Interactive AB

The complainants
See appendix 1 and 2

National ref. no.:
DI-2021-3401

Case register
128349

Date:
2025-05-07

Decision in under the GDPR – Paradox Interactive AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection (IMY) concludes that Paradox Interactive AB (publ) (556667-4759) (the company) has failed to fulfil its obligation under Article 13(1)(c) and Article 12(2) of the General Data Protection Regulation (GDPR or Regulation)[1] by not properly informing the complainants of the legal basis for the processing of personal data when the personal data was collected, and by not facilitating the exercise of data subject's rights under the Regulation.

IMY gives Paradox Interactive AB (publ) a reprimand pursuant to Article 58(2)(b) of the Regulation.

Presentation of the supervisory case

IMY has received two complaints from the company in accordance with the provisions on the competence of the lead supervisory authority in Article 56 of the GDPR. One of the complaints (complaint 1)[2] has been submitted to IMY by one of the German DPAs and the other complaint (complaint 2)[3] has been submitted by the Finnish DPA.

IMY has initiated supervision of the company in order to review the personal data processing covered by the complaints.

The case was dealt with by exchange of letters. Due to the cross-border nature of the supervisory case, IMY has made use of the cooperation and consistency mechanisms provided for in Chapter VII of the GDPR. Relevant supervisory authorities have been the data protection authorities of Finland, Portugal, Germany, Poland, Norway,

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
08-657 61 00

[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 the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[2] National ref. no. in Germany: 4400-6/83.
[3] National ref. no. in Finland: 3922/163/2019

Belgium, the Netherlands, Italy, Luxembourg, Denmark, France, Hungary, Austria, Slovakia, Slovenia, Ireland, Spain, Greece and Latvia.

What the parties have put forward

Complainant 1 essentially puts forward the following.

In order to start the games provided by the company, it is necessary to accept an end-user agreement for the company's start-up program. There is no possibility to refuse the processing of personal data. The Company's terms and conditions do not contain any information on how to withdraw consent.

It is not clear what data the launcher collects. Some users have indicated that the launcher requests to collect keyboard presses, which raises the question of whether it collects keyboard press data also outside the games. It is unclear how the company handles the data on keyboard presses.

Paradox's privacy policy and list of recipients indicate a large number of companies that receive the personal data that the company collects. It does not appear that the company adheres to the principle of data minimisation. In most cases, the legal basis for the transfer appears to be legitimate interests, which is questionable. Furthermore, it is questionable whether it is justified to share data on which games a particular user has purchased with advertising companies, such as Google Ads and Mailchimp. Finally, it is doubtful how information about the playing of a game that is already fully developed can be justified for future development.

Complainant 2 essentially puts forward the following.

In order to play one of the company's games, you must agree to a long privacy policy. It is not possible to refuse the processing of personal data. The Company processes a large amount of personal data. However, it is only vaguely described what information is collected and for what purposes. Paradox collects more data than is needed to provide the games.

He has contacted the company and requested information on what personal data is collected about him and has indicated that he does not want any of his personal data to be collected. The company has not dealt with his request and has referred him to the company’s customer centre and forum.

The company essentially puts forward the following.

The launcher does not collect keyboard presses. The request for permission to collect keyboard presses that were sent to some players was due to an error in the configuration of the launcher in relation to Apple's new update. The error was fixed in March 2020.

The end-user agreement is a way of informing the complainant about how his personal data will be processed in connection with the use of the launcher. It is not a way for the company to collect the complainant’s consent for the processing of his personal data. The End User Agreement states that the terms of the Privacy Policy are accepted by accepting the End User Agreement. This is an incorrect description. The Company will update its End User License Agreement to avoid misunderstandings. The legal basis for the processing in this case is the performance of a contract and legitimate interest.

The company has instructed the complainant to log in in order to identify himself and make a request for information and deletion via the company's system. This is to ensure that the request is made in a secure manner by the person to whom the personal data actually belongs. It is not possible for the company to identify the complainant on the basis of the email address alone. The company has not been able to act on any request under the GDPR because the complainant has chosen not to identify itself.

Reasons for the decision

Applicable provisions, etc.

It follows from Article 57(1)(f) of the GDPR that IMY must process complaints from data subjects who consider that their personal data are being processed in a manner contrary to the GDPR. It is also apparent from that provision that IMY is to examine, where appropriate, the subject matter of the complaint.

Article 5 of the GDPR sets out the basic principles governing the processing of personal data. The principle of data minimisation set out in Article 5(1)(c) requires that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are processed.

It follows from Article 13(1)(c) of the GDPR that, where personal data are collected from the data subject, the controller must inform the data subject of the legal basis for the processing.

The legal bases are set out in Article 6 of the GDPR. Article 6(1)(b) states that processing is lawful if it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. Article 6(1)(c) states that processing is lawful if it is necessary for compliance with a legal obligation to which the controller is subject. Article 6(1)(a) states that processing is lawful if the data subject has given his or her consent to the processing of his or her personal data for one or more specific purposes. The definition of consent is set out in Article 4(11) of the GDPR and Article 7 sets out the conditions for valid consent.

The rights of data subjects (persons whose personal data are processed) are set out in Chapter III of the GDPR. Under Article 15 of the GDPR, the data subject has the right to obtain information from the controller as to which personal data concerning him or her are being processed (right of access). According to Article 17 of the GDPR, the data subject has the right to erasure of his or her personal data in certain cases. Article 21(1) provides, inter alia, that the data subject has the right to object to the processing of his or her personal data if the processing is based on a legitimate interest and the reasons for the objection relate to his or her particular situation.

It follows from Article 12(6) of the GDPR that the controller may request the necessary information from the person making the request pursuant to, inter alia, Articles 15, 17 and 21 to confirm his or her identity, if the controller has reasonable grounds to doubt the identity of the person making the request.

Article 12(2) reads as follows: The controller shall facilitate the exercise of the rights of the data subject in accordance with Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to comply with the data subject's request to

exercise his or her rights under Articles 15 to 22, unless the controller demonstrates that he or she is not in a position to identify the data subject.

IMY's assessment

Keyboard presses
Complainant 1 submits that, through the launcher, the company collects data on keyboard presses. The company has stated that the launcher does not collect keyboard presses. Nothing has come to light in the investigation that gives IMY reason to question the company's information. There is therefore no reason to find any infringement under the GDPR in this regard.

Information to data subjects
The complainants have argued that, in order to start the games provided by the company, they have had to accept that the company processes personal data in accordance with its privacy policy. Complainant 1 has argued that there is a lack of information on how to withdraw consent. The complainants further submit that the company's information to the data subjects is unclear and vaguely worded.

The company has stated that the actual legal basis for the personal data processing in question is the fulfilment of agreements and legitimate interest. The Company acknowledges that the End User Agreement incorrectly states that the complainants accept the terms of the Privacy Policy by accepting the Agreement.

IMY considers that the information that the complainants received when the personal data was collected was designed in such a way that it has erroneously appeared that the legal basis was consent under Article 6(1)(a) of the GDPR. In fact, the processing of personal data at issue was based on other legal bases. IMY therefore considers that it has failed to fulfil its obligation under Article 13(1)(c) of the GDPR by failing to correctly inform the complainant of the legal basis for the processing of personal data at the time when the personal data were collected.

In view of the company's statement that the processing of personal data at issue in the main proceedings is not based on consent, IMY has no reason to investigate whether the complainant was able to withdraw the consent and was informed of that possibility. IMY further considers that, given the nature of the case, it is not appropriate in the present case to investigate whether the privacy policy otherwise meets all the requirements of Article 13 of the GDPR. That assessment is made, inter alia, in the light of the time which has elapsed since the complaints were lodged and the fact that the complaints do not indicate in a sufficiently specific manner in the complaint file how the company failed to fulfil its obligation to provide information.

Legal basis and principle of data minimisation
Complainant 1 submits that a large number of recipients receive the personal data that the company collects and that it does not appear that the company complies with the principle of data minimisation. Complainant 1 also questions whether the company has had a legitimate interest in the processing. Complainant 2 has argued that the company collects more data than is necessary to provide the games.

IMY has asked questions about the company's various personal data processing operations, its purposes and legal bases. The company has submitted a large amount of information about the personal data processing in question and has submitted material in support of its tasks.

IMY considers that, given the nature of the case, it is not appropriate in the present case to investigate whether each individual processing of personal data has a legal basis and is compatible with the principle of data minimisation. The assessment is made taking into account, in particular, the time that has elapsed since the complaints were lodged, the large amount of information that has been received in the case and the lack of sufficiently concrete indications (either in the complaint file or in the material provided by the company) that the complainants' personal data have been processed without a legal basis. In light of the above, IMY concludes that there is no infringement under the GDPR in this part.

Rights of data subjects
Complainant 2 submits that the company did not deal with his request for information and objection to not having his personal data processed, but referred him to the company's customer centre and forum.

The complainant states that it has been instructed to log in in order to identify itself and to make a request via the complainant's system. This is to ensure that the request is made in a secure manner by the person to whom the personal data actually belongs.

It is apparent from the documents submitted by the complainant, inter alia, that the company gave him the following reply. "We have introduced this requirement because we need to be able to verify that you are the actual account owner and login will ensure that this is the case. This is particularly important for GDPR-related issues as such requests will contain personal information' (IMY translation in English).

IMY notes at the outset that the GDPR does not contain any formal requirements as to how a request from a data subject who wishes to exercise his or her rights under the GDPR is to be made. Where a data subject makes a request using a communication channel provided by the controller, the controller shall handle such a request, even if the controller prefers another channel.[4]

At the same time, in order to ensure secure processing and minimise the risk of unauthorised disclosure of personal data, a controller must be able to ascertain which data relate to the person (identification) and confirm the identity of the person (authentication) in cases where someone requests access to their personal data.[5] For these situations, the controller may, for example, put in place a secure channel for data subjects to provide additional information. However, where the controller imposes burdensome measures aimed at authenticating the data subject, it must provide adequate justification and ensure compliance with all fundamental principles of the GDPR, as well as compliance with the obligation to facilitate the exercise of the data subject's rights under Article 12(2) of the GDPR.[6]

IMY makes the following assessment. It is clear only that the complainant has approached such a channel of communication provided by the company in order to make its request. The company has therefore been obliged to handle the request. On the basis of the information in the file, it is unclear what kind of request the complainant has made. Admittedly, in the event of a request for access under Article 15 of the GDPR, the company may have had reason to refer the complainant to its authentication system in order to minimise the risk of unauthorised disclosure of

[4] Stockholm Administrative Court of Appeal judgment of 7 June 2024 in case No 2639-23 and European Data Protection Board (EDPB) Guidelines 01/2022 on data subjects' rights – right of access, version 2.1, p. 52 et seq.
[5] EDPB, 01/2022, p. 58.
[6] Cf. EDPB, 01/2022, p. 70 f.

personal data. However, in the case of an objection to certain processing operations under Article 21 of the GDPR or a request for the type of general information referred to in Article 13 of the GDPR, IMY notes that there is normally no reason to authenticate, and sometimes even to identify, the data subject in order to satisfy the objection or request for information.

IMY makes the following assessment. The company has not sufficiently justified the existence of such a type of request that authentication of the complainant was necessary. Furthermore, the company has not taken any steps to clarify the nature of the request, provided the complainant with general information that does not require authentication or taken any other steps to facilitate the exercise of its rights.

IMY therefore considers that the company has failed to fulfil its obligation to facilitate the exercise of the complainant 2's rights under Article 12(2) of the GDPR by responding to the complainant's request with a reference to its authentication system.

Choice of intervention

IMY has found above that it has failed to fulfil its obligations under Article 13(1)(c) and Article 12(2) of the GDPR. The last question to be considered by IMY is what action should be taken in response to the infringement.

In the event of infringements of the GDPR, IMY has a number of corrective powers, including reprimands, injunctions and fines. It follows from Article 58(2)(a) to (j) of the GDPR. According to recital 129 of the GDPR, IMY must take such measures as are appropriate, necessary and proportionate to ensure compliance with the GDPR.

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 instead of the other measures referred to in Article 58(2), such as injunctions and prohibitions. In the case of a minor infringement, IMY may, as stated in recital 148 of the GDPR, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and previous relevant infringements, must be taken into account.

IMY notes that the current investigation is based on two individual complaints. It has been four and five years since the complaints were lodged with the German and Finnish data protection authorities respectively. The infringement is not considered to be of a serious nature. The company has not previously been found to have infringed the General Data Protection Regulation.

On an overall assessment of the above circumstances, IMY considers that there is a minor infringement as referred to in recital 148 of the GDPR. The company must therefore be granted a reprimand pursuant to Article 58(2)(b) of the GDPR.

This decision was made by the Head of Unit [redacted], following a presentation by the legal officer [redacted].

[redacted]

Appendixes

1. Personal data of complainant 1
2. Personal data of complainant 2

How to appeal

If you wish to appeal the decision, write to the Swedish Authority for Privacy Protection (IMY). Indicate in the letter which decision you wish to appeal and the change you request. IMY must receive the decision no later than three weeks from the day you received it. If the appeal is lodged in time, IMY will then forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to IMY if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. IMY's contact information is shown on the first page of the decision.

Swedish Authority for Privacy Protection

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's draft decision.

Swedish ref no:
DI-2021-3401

Case register:
128349

Date of the draft decision:
2025-05-07

Appendix 1 to decision under the GDPR – The personal data of the complainant

Name: [redacted]

Address: [redacted]

E-mail: [redacted]

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
eu@imy.se

Telephone:
08-657 61 00

Swedish Authority for Privacy Protection

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's draft decision.

Swedish ref no:
DI-2021-3401

Case register:
128349

Date of the draft decision:
2025-05-07

Appendix 2 to decision under the GDPR – The personal data of the complainant

Name: [redacted]

E-mail [redacted]

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
eu@imy.se

Telephone:
08-657 61 00