noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
Austria

Datenschutzbehörde (DSB)
Barichgasse 40-42
1030 Wien

Per E-Mail: dsb@dsb.gv.at

Vienna, 24.04.2025

noyb Case-No: C-098

Complainant: [redacted]

represented under Article 80(1) DSGVO by: *noyb* – European Center for Digital Rights
Goldschlagstraße 172/4/3/2, 1140 Vienna

Respondent: **Ubisoft Entertainment SA**
28 Rue Armand Carrel, 93100, France

Regarding: Article 6 GDPR

COMPLAINT

1. REPRESENTATION

1. *noyb* – European Center for Digital Rights is a not-for-profit organisation active in the field of the protection of data subjects' rights and freedoms with its registered office in Goldschlagstraße 172/4/2, 1140 Vienna, Austria, registry number ZVR: 1354838270 (hereinafter: *„noyb"*) (**Attachment 1**).

2. *noyb* is representing [redacted] (the complainant) under Article 80(1) GDPR (**Attachment 2**).

2. SUMMARY

3. This complaint pertains to the business practice of Ubisoft (the controller), regarding their unlawful data collection when people play single player games.

4. It all started when the complainant found that they could not launch a single player video game they owned without first connecting to the internet. They also found that the controller collected data from them during their play session.

5. There is no valid legal basis for this data collection under Article 6 of the GDPR.

6. The complainant therefore requests that the Data Protection Authority exercises its corrective measures to ensure the controller brings the data processing in line with the GDPR and that it imposes a fine as a punitive measure and to ensure effective enforcement of the regulation.

3. FACTS PERTAINING TO THE CASE

3.1. Background

7. The controller is a video game producer and publisher of several popular video game franchises. Among them Assassins Creed, the Crew, Prince of Persia and Rainbow Six. They are one of the largest video game companies established in Europe, with a revenue of over two billion € a year.[1]

8. The video game published by the controller, that the complainant played most recently is Far Cry Primal. This game is a single player game, meaning that the complainant cannot interact with other players in any way when playing the game.[2]

[1] https://companiesmarketcap.com/eur/ubisoft/revenue/ (2025-04-23)

[2] In attachment 7 (traffic_game_data).csv further information about games that the controller's published that the data subject has enjoyed, or at least played, can be discerned.

9. The game requires the user to log in to a Ubisoft account to launch even though the game has no online features.

10. The function of the video game is akin to a board game, that you can only play alone.

3.1.1. *The complainant identifies data transfers*

11. The complainant played the game Far Cry Primal (the game), a game published by the controller, on the 13st of September 2024. The complainant had purchased the game through the online marketplace Steam. When trying to launch the game off-line, the complainant noticed that this was not possible. Rather the game forced them to log into a Ubisoft account to launch the game.

12. The complainant was astonished that it was impossible to play a single player game, offering no online functionalities, off-line. Curious as to what the kind of information the controller collected about them, the complainant requested access from the controller. In the attached file uplay_traffic_data.csv[3] it can be seen that the controller knows when the complainant, identified by their user ID: [redacted], launched the game, when they quit playing and exactly how long they kept the game running.

13. Being a tech-savvy individual, the complainant additionally examined what kind of data packages were being sent to the controller when playing the game (the data processing operation), and so they started the game again and had it running for about 10 minutes.[4] They discovered that 150 unique DNS packages (queries and responses) were sent during this time and they identified 56 requests to initiate a connection between the complainants computer and external servers.[5]

14. From the network traffic captured by the complainant it can be inferred that the controller, Google, Amazon and Datadog (among others) are recipients of the complainant's data.

15. Some of the data transfers are labelled "metrics" and the controller seems to be responsible for this network traffic.

16. It is however not apparent what data is sent since the transmissions were encrypted using TLS (transport layer security).

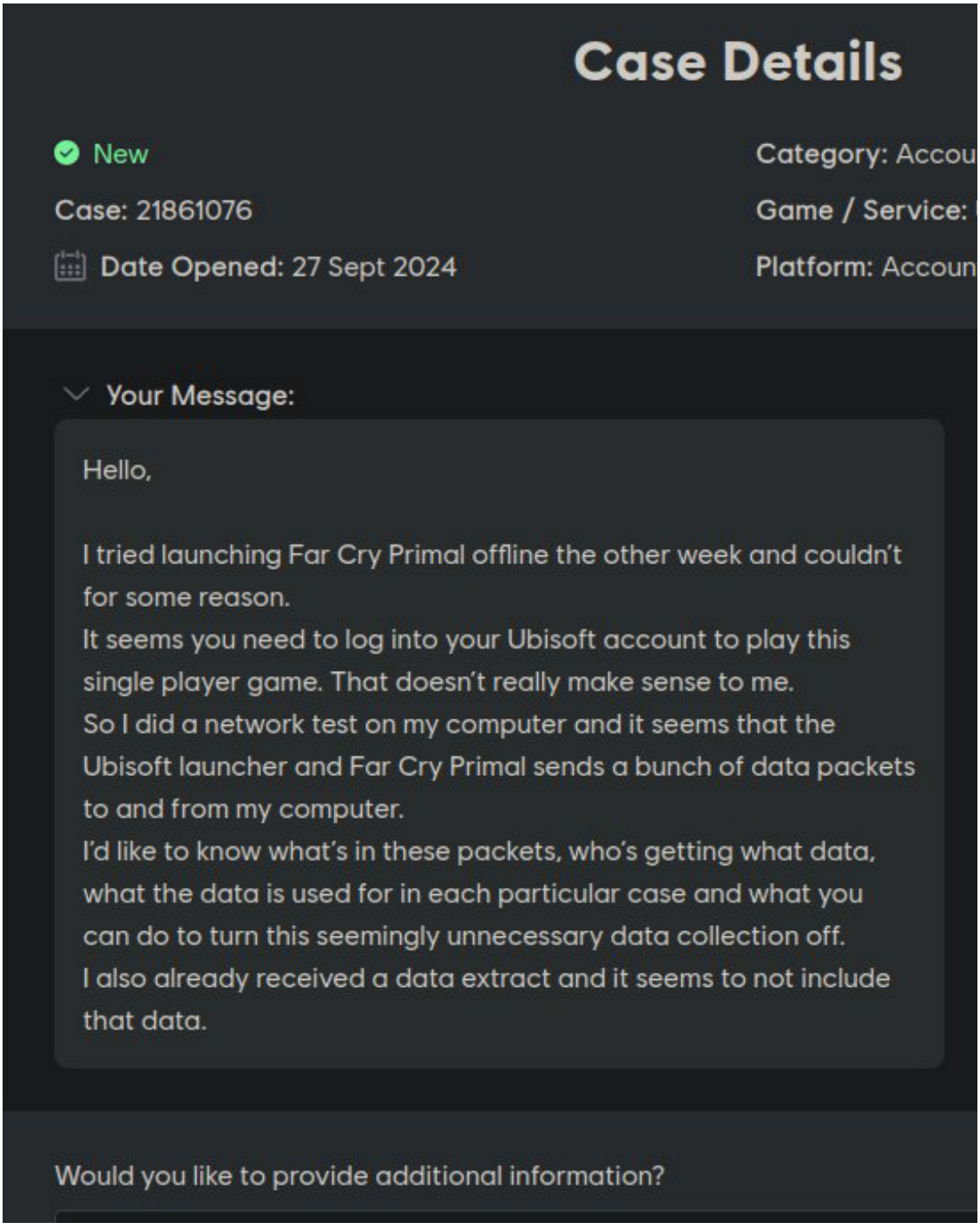
[3] See attachment 3 (uplay_traffic_data).csv

[4] See attachment 4 (far_cry_primal).pcap

[5] A selection of data packets identified as sent or received have been compiled in attachment 12

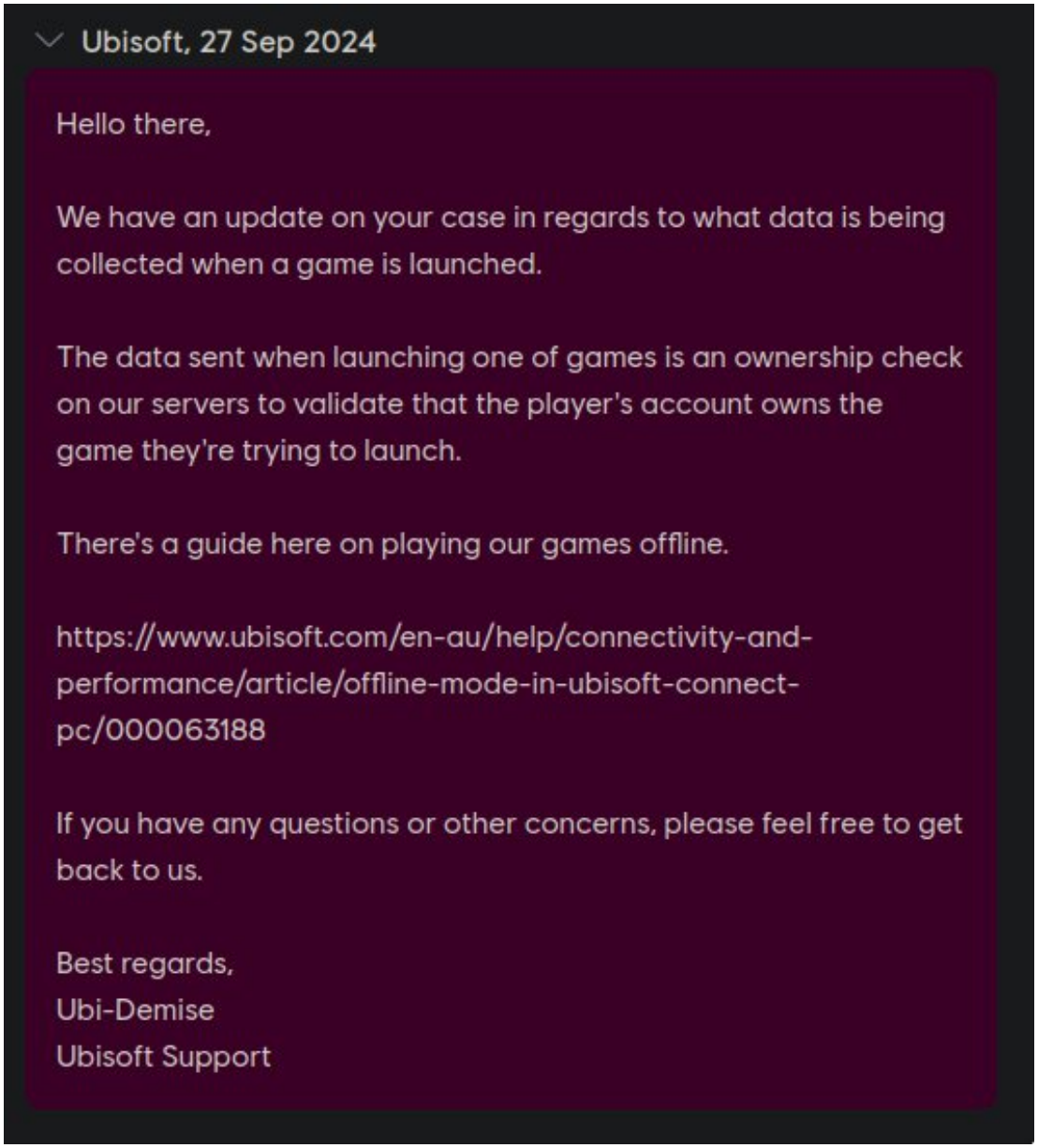
3.1.2. *Contacting customer support*

17. On the 27th of September 2024 the data subject contacted the controller's customer support with the following inquiry:[6]



[6] attachment 13 (data protection inquiry)

18. After a bit of a back and forth,[7] the controller replied as follows:[8]



19. What is noteworthy about this reply is that only information about the launch of the game is provided. No explanation regarding what data is collected for metrics or why data packets are sent back and forth between the player and, for example, Google servers when the player is playing the game.

20. Some indication as to what data and why data is collected might however be found in the End User License Agreement and/or the Privacy Policy of the controller.

---

[7] attachment 15 (conversation with support).zip

[8] attachment 14 (data protection reply).png

3.2. End User License Agreement and Privacy Policy

21. In the End User License Agreement of the controller (EULA[9]), relating to the video game in question, the controller confirms that they collect personal data *"in order to provide You with a better game experience"*[10] as well as that they use *"third party analytics tools to collect information concerning your and other users' gaming habits and use of the product"*[11]. The data collected in the latter case is not considered personal data by the controller.[12]

22. The Privacy Policy of the controller in turn explains that the controller *collects "**game data**, to **improve your experience** and the **security of our services**"*[13] as well as *"**login and browsing data**, to **enable the operation** and **security of our Services**"*[14].

23. Offering the player *"the **best possible user experience**, such as to ensure the **security of the Services**"* is in the Privacy Policy expressed as a legitimate interest of the controller.[15]

24. The complainant, and all other users of the games provided by the controller do not have an option to choose whether the data processing as described above will be conducted or not. Rather the complainant is considered, by the controller, to accept the conditions set out in the EULA and Privacy Policy simply by interacting with the product.[16]

4. GROUNDS FOR THE COMPLAINT

4.1 The information collected is personal data

25. Contrary to the claims of the controller[17] the data collected from the complainant is personal data. CJEU C-604/22:

> *"43. Even if a TC String did not itself contain factors allowing the data subject to be identified directly, it would still be the case, in the first place, that it contained the individual preferences of a specific user regarding his or her consent to the processing of personal data concerning him or her, that information 'relating to [a] ... natural person' within the meaning of Article 4(1) of the GDPR"*
>
> *"45. In so far as associating a string composed of a combination of letters and characters, such as the TC String, with additional data, inter alia with the IP address of a user's device or with other identifiers, allows that user to be identified, it must be considered that the TC String contains information concerning an identifiable user and therefore constitutes personal data within the meaning of Article 4(1) of the GDPR, a conclusion which is supported by recital 30 of the GDPR, which expressly refers to such a case."*

---

[9] Attachment 5 (Ubisoft EULA (24-09-23)).htm

[10] See section 3.2(b) of attachment 5 (Ubisoft EULA (24-09-23)).htm and associated files

[11] See section 3.2(c) of attachment 5 (Ubisoft EULA (24-09-23)).htm and associated files

[12] See section 3.2(c) of attachment 5 (Ubisoft EULA (24-09-23)).htm and associated files where the controller states the following *"Standing alone, this information is not personal data"*

[13] See section 3.d) of attachment 6 (Ubisoft Privacy Policy (2024-09-16)).htm and associated files

[14] See section 3.d) of attachment 6 (Ubisoft Privacy Policy (2024-09-16)).htm and associated files

[15] See section 7. of attachment 6 (Ubisoft Privacy Policy (2024-09-16)).htm and associated files

[16] "By installing or using the Product, You agree to accept and to be bound by (1) this EULA and (2) the Privacy Policy at all time." See attachment 5 (Ubisoft EULA (24-09-23)).htm and associated files

[17] See section 3.2(c) of attachment 5 (Ubisoft EULA (24-09-23)).htm and associated files

26. This interpretation by the CJEU falls well in line with the definition of personal data in Article 4(1) of the GDPR where personal data is clearly defined as "*any information relating to and identified or identifiable natural person*". It also clarifies that an identifiable natural person does not have to be directly identifiable by the data in question for that data to be personal data. It is enough that the data can be combined with something else for the data to be personal.

27. From the EULA of the controller the following can be read: *"The information collected may contain the following, without limitation:* ***mobile device unique identity or other device identifiers*** *and settings, carrier, operating system****, localization information, date and time spent on the Product****, game scores, game metrics*** *and statistics, feature usage,* ***advertising conversion rates, monetization rate, purchase history*** *and other similar information".*

28. The highlighted sections is information that clearly relates to the complainant, either directly or indirectly.

29. In the controllers own words the data collected does not constitute personal data "*standing alone*"[18] but that it will be treated as personal data if combined with personal data. Which in light of the CJEU judgement cited above means that the data is personal data regardless of whether the combining happens or not. It is enough that the data can be combined with a direct identifier for the data to fall under the definition of personal data under Article 4.

4.2. Data is processed unlawfully

4.2.1. Game can be run off-line so data collection is not necessary

30. Considering that the complainant at no point consented to having his data processed when he played the game, and that the data processed is personal data, one of the other legal bases for data processing under Article 6(1) GDPR must apply for the data processing operations conducted to be legal.

31. Despite the passage in the EULA postulating that by playing the game the user accepts the privacy policy the mere playing does not constitute consent within the meaning of Article 4(11) GDPR. The playing does neither indicate agreement to a data protection policy nor would this be informed, as prior to the playing no information on the consequences regarding the processing by the controller was given.[19]

32. The common condition among the legal bases' other than consent is that the data processing operation in question must be <u>necessary</u> to fulfil the purpose of the processing activity in question.

33. In the words of the CJEU:

> "[…] *with regard to the condition that the processing of personal data be necessary for the purposes of the legitimate interests pursued, that condition requires the referring court to ascertain that the*

[18] See section 3.2(c) of attachment 5 (Ubisoft EULA (24-09-23)).htm and associated files

[19] Regarding this see the procedure preceding CJEU, 11.07.2024, C-757/22 (Regional Court of Berlin, 28.10.2014 - 16 O 60/13).

> *legitimate data processing interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter (see, to that effect, judgment of 22 June 2021, Latvijas Republikas Saeima (Penalty points), C-439/19, EU:C:2021:504, paragraph 110 and the case-law cited)."*[20]

34. Or to express it more succinctly: a data processing operation is not necessary when there are less invasive means available to serve the same end. Essentially the necessity condition in Article 6 is an expression of the data minimisation principle in Article 5(1)(c) GDPR.[21] This principle in itself can be considered an expression of legislative proportionality,[22] where the processing of data in the controller's self interest isn't forbidden but simply subject to the condition of not being too extensive for the envisaged purpose of the data processing.

35. The only claim of the controller, when asked, is that the data processing identified by the complainant is necessary to verify ownership of the game.[23]

36. *First*, this can't be necessary as the complainant has bought their game through the online marketplace Steam, which already verifies ownership by selling game licenses directly or verifies game licenses sold by third party vendors.[24]

37. *Second*, the controller itself explained that it does provide a (hidden) off-line option (see above, response by Ubisoft in § 18). If the game is launched off-line, verification of ownership would not be possible. It cannot be true that the proof of ownership is "necessary" when the data subject is connected to the internet, but for some reason not when they are not online. The alternative to play the game off-line, thus eliminating the possibility for the controller to collect data from the data subject, clearly shows that the claim regarding verifying ownership is non-sensical. Furthermore if running the game off-line is a viable option to play the game as the controller claims.[25] It can't be necessary to process data as the game is running for any reason listed in Article 6(1)(b) to (f) GDPR.

38. *Third*, even if verification was necessary, the explanation provided by the controller does not provide an explanation as to why data was collected from the complainant as the game was running and not just once at the launch of the game.[26] The controller's explanation also doesn't explain or justify the transfer of personal data to other entities like Google, Amazon and Datadog (see paragraph 14 above).

39. In short: The purchase is verified by a third party making further verification by the controller unnecessary. If the game can be run off-line "verification" cannot be "*necessary*" since this

---

[20] Se Case C-252/21 paragraph 108

[21] See Opinion 01/2024 Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, page 12, attachment 8 (edpb_guidelines_202401_legitimateinterest_en).pdf.

[22] See article 52 of the Charter

[23] See attachment 14 (data protection reply).png

[24] Games purchased through Steam also generally needs to be run through Steam as a launcher, and while connected to the internet, the first time the game is launched, as can be seen in the Steam FAQ here: https://help.steampowered.com/en/faqs/view/0E18-319B-E34B-B2C8 2025-04-09)

[25] See attachment 14 (data protection reply).png

[26] See attachment 4 (far_cry_primal).pcap and section 3.2.b-c of attachment 5 (Ubisoft EULA (24-09-23)).htm

prohibits data collection by the controller. Lastly "verification" does not explain why data is collected from the data subjects at any other point other than at the launch of the game.

4.2.2. Consent necessary to access terminal equipment

40. It should be noted that, under Article 5(3) of the e-Privacy Directive 2002/58, collecting data from the user's terminal equipment requires consent from the user unless the collection is necessary to provide the service to the user (regardless of whether the data collected is personal data or not).[27] The latter which in GDPR terms would mean that collection of (personal) data from the complainants computer would have to be necessary to fulfil a contractual obligation of the controller to be allowed under Article 6 of the GDPR. Something which is not applicable in this case since the game offers no online functionality.

4.3. Legitimacy of the processing and the balance of interest

4.3.1. Claims of the controller

41. Outside of the dialogue the data subject has had with the controller, the controller seems to claim that the data collection at hand is necessary for product improvement and security purposes, as expressed in the Privacy Policy[28] and for analytics and ad serving as expressed in the EULA[29]. No other purpose mentioned in the controller's EULA or privacy statement seems even remotely applicable for this processing activity. The product improvement and security purposes are expressed as a legitimate interest of the controller. The purpose of the analytics and ad serving are never explained.

42. If the claims of the controller would mean that data processing is necessary, it should be noted that the processing activities that the controller claims that they conduct still fall short of the requirements in Article 6(1) GDRP.

4.3.2. Analytics and Ad Serving

43. It is self-evident that analytics and ad serving can't be based on any legal basis expressed in Article 6(1) GDPR other than the complainant's consent (which was never given) or for the pursuit of a legitimate interest, of the controller or third party. Since consent for the data processing was never given, it must be assumed that the analytics and ad serving is done in the controller's interest. However, since that interest is never expressed or explained by the controller the interest cannot be legitimate.[30]

---

[27] See DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) Article 5(3).

[28] attachment 6 (Ubisoft Privacy Policy (2024-09-16)).htm

[29] attachment 5 (Ubisoft EULA (24-09-23)).htm

[30] See section 3.2.c of attachment 5 (Ubisoft EULA (24-09-23)).htm and paragraph 17 of attachment 8 (edpb_guidelines_202401_legitimateinterest_en).pdf

4.3.3. Product improvement

44. Similarly the product improvement purpose is expressed by the controller in a nebulous way: *"to offer you the best possible user experience"*.[31] It is unclear from the wording how this is an interest of the controller, as the interest expressed seems to be the complainants interest and not the controllers, or if it's detached from processing data for security purposes.[32] The generic interest in improving the product is therefore not a legitimate interest.

45. The product improvement interest is also not real and present as the game has been sold "*as is*" by the controller.[33] By their own admission the consumer should therefore not expect them to improve the game, as they have no expressed incentive to do so. The exception to this lack of interest being to fix bugs and crashes, as the game not being in a functional state might warrant a refund from consumers.

46. However, voluntary bug/crash reporting is an industry norm.[34] It is therefore demonstrably proven that automated bug/crash reporting is not necessary to achieve the objective at hand. Giving the data subject power to decide if they want to report bugs and crashes falls in line with the CJEU's ruling in C-621/21.[35]

47. Lastly it should be concluded that there is no reason for the complainant to expect that the controller collects their data as they play what is ostensibly a solitary experience. Similar to playing Solitaire or solving a Sudoku. Having their playtime monitored by the controller therefore seems a disproportionate infringement of the private sphere of the complainant.

4.3.4. Security purpose

48. It should be noted that processing personal data in the controller's security interest can only be necessary if there is some kind of interaction between the data subject and the controller that could be subject to security issues. This connection, however, is only created by the collection of the data subject's data. If no data is collected, and no connection between the data subject and the controller is established, there is no security risk associated with the connection.

49. The security interest therefore hinges on the other reasons for the data processing operation expressed by the controller fulfilling the conditions of Article 6(1). Since they do not, the processing personal data in pursuit of security also cannot fulfil the conditions in Article 6(1).

---

[31] See section 7 of attachment 6 (Ubisoft Privacy Policy (2024-09-16)).htm

[32] The security of the service seems to be listed as an example of providing the best possible user experience: "[…] offer you the best possible user experience, such as to ensure the security of the Services", see section 7 of attachment 6 (Ubisoft Privacy Policy (2024-09-16)).htm

[33] See section 6 attachment 5 (Ubisoft EULA (24-09-23)).htm

[34] See attachment 9 and 10 crash reporters from Paradox and Larian respectively

[35] See Case C-621/22, Koninklijke Nederlandse Lawn Tennisbond, para. 51

4.3.5. Balancing test

50. Even if the interests above could be considered legitimate and the processing would be necessary to achieve the pursued interest, it should be noted that the controller has not taken the interests of the complainant or other data subjects into account when committing to the data collection identified by the complainant. At least not in a way expressed by the controller in accordance with their obligations in Article 13 GDPR.

51. Crucial in the balancing test is to recognize that collecting data from the data subject, as they play a video game, is tantamount to monitoring their behaviour in their private sphere. The controller has not considered that the complainant might not want to be monitored, especially not secretly. Due to the inadequate information provided to the data subject it is not even possible to assess the scope and type of collected data. Unless a connection between the controller and the complainant is strictly necessary for the service, this kind of violation of the data subject's privacy and intrusion into the private life can only be considered a direct violation of the data subjects right to respect for his private life and home as expressed in Article 7 of the Charter and of his right to protection of personal data under Article 8 of the Charter.

52. If you want to enter someone's home, you should be invited, otherwise you're trespassing. If the behaviour is illegal in the physical sphere, it should be illegal in the digital one as well. There is no reason to apply a different standard.

53. The balancing test thus necessitates that the controller asks the data subject for permission to enter their computer. Just like how Ingvar Kamprad[36] needs to knock if he wants to know how I put together my Billy.

5. REQUESTS AND SUGGESTIONS

5.2. Request to investigate

54. The complainant hereby requests the competent Data Protection Authority to duly, thoroughly and timely investigate the data processing practices of the controller in relation with video games.

5.3. Request for a declaratory decision and effective corrective measures

55. The complaint hereby requests the competent Data Protection Authority to

    - to declare that the controller infringed upon Article 6(1) GDPR in conjunction with Article 5(1)(a) GDPR by processing personal data of the complainant without a valid legal basis.

    - order the controller to delete all personal data of the complainant processed without a valid legal basis in accordance with Article 17(1)(d) GDPR.

[36] The founder of IKEA https://en.wikipedia.org/wiki/Ingvar_Kamprad

- impose a ban on the processing of personal data of the complainant insofar it cannot be based on a valid legal basis.

5.4. Suggestion to impose a general order

56. The complainant hereby suggests that the competent Data Protection Authority order the controller to bring its data processing in compliance with the provisions of the GDPR.

5.5. Suggestion to impose a fine

57. Given that millions of users are affected by the practices of the controller the complainant hereby suggests to the competent Data Protection Authority to impose an administrative fine upon the controller.

6. CONTACT

58. Communications between *noyb* and the Competent Supervisory Authority in the course of this procedure can be done by email at [redacted] with reference to the **Case-No C-098** or [redacted].