Information and Data Protection Commissioner

[redacted]

vs

[redacted]

COMPLAINT

1. On the 30th October 2020, Mr [redacted] (the "**complainant**") lodged a complaint with the Berlin Commissioner for Data Protection and Freedom of Information (the "**Berlin SA**") against [redacted][1], trading as [redacted] (the "**controller**").

2. The Berlin SA lodged a mutual assistance notification under article 61 of the General Data Protection Regulation[2] (the "**Regulation**"), wherein the Information and Data Protection Commissioner (the "**Commissioner**") acted in its capacity as the lead supervisory authority. In this context, the Berlin SA forwarded to the Commissioner a translated copy of the initial complaint and of the evidence attached thereto.

3. From the analysis of the documentation received, it transpires that, on the 22nd September 2020, the complainant exercised the right to access his personal data with the controller in terms of article 15 of the Regulation. On the same day, the controller responded to the complainant requesting him to submit a certified copy of his identity card or passport.

[1] [redacted]

[2] 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.

4. On the 22nd September 2020, the complainant provided the controller with a photo of his identity card and held that in his views there were no grounds for requesting a certified copy of the document.

5. In subsequent e-mail exchanges between the controller and the complainant, the controller sustained that a certified copy of the complainant's identity card was necessary for identity verification purposes, considering that the complainant's request involved the transmission of sensitive data. On the other hand, the complainant observed that, according to him, the request for a certified copy of his identity card for identity verification purposes was unlawful and ran contrary to the Regulation. The complainant further added that, for the purpose of confirming his identity, the controller should have used other information in its possession, such as his e-mail address.

INVESTIGATION

6. On the 28th January 2021, pursuant to article 58(1) of the Regulation, the Commissioner requested the controller to provide its submissions in relation to the allegations raised by the complainant. Within this context, the Commissioner requested the controller to submit (i) a copy of the policy to identify and verify the identity of subscribers; (ii) reference to any legal basis to require additional information /documents to confirm subscriber's identity; and (iii) any specific reason why the complainant was requested to provide further information / documents to confirm his identity. In terms of this Office's internal investigation procedure, the controller was provided with a copy of the complaint together with the supporting documents attacted thereto.

7. By means of an e-mail dated the 2nd February 2021, the controller submitted the following principal legal arguments for the Commissioner to take into consideration during the legal analysis of the case:

    i. that the controller receives "*several false requests from fraudsters trying to get users data*" by "*trying to mimic our players email address, or their close relatives to use our client's emails*", thus the controller needs to adopt additional measures to verify players' authenticity, including requesting proof of identity;

ii. that "[o]*ccasionally or in case our customer support agents are not fully satisfied, we do request additional method of verification, that is a certified or notarized copy*" of users' identification documents, and this was defined in recital 64 of the Regulation as "*identity verification*";

iii. that the last communication with the complainant was on the 30th October 2020, when the complainant "*was advised by a customer support agent that his request would be escalated to the relevant department and the request was forwarded 9to Floor Manager*";

iv. that "[a]*ccording to* [the controller's] *procedures the case remains open for 30 days and if the request is not processed further it closes as "Case Closed - Player did not provide required ID within 30 days'*"";

v. that "*the data subject* [has] *multiple accounts with us, we do require that his identity be verified to process his GDPR request*"; and

the controller provided a copy of the procedure "*Managing Personal Data Requests Procedure*" dated the 30th April 2020 and approved by the company CEO, a file entitled "*Examples of fraudulent cases*" and copy of a Power Point presentation entitled "*GDPR Guidelines and Processes*".

8. On the 2nd February 2021, with reference to the controller's claim that the complainant had multiple accounts with the controller, the Commissioner requested the controller to specify: (i) why having multiple accounts was considered a valid reason to require additional proof of identity; (ii) whether all the complainant's accounts were under the online casino [redacted] or with other casinos operated by the controller; (iii) whether the complainant filed the right of access request for all his accounts or for a specific account; and (iv) whether the e-mail address from which the controller received the right of access request was the same e-mail address that the complainant used to register his account on the online casino(s) or otherwise.

9. On the 4th February 2021, the controller informed the Commissioner, that "[l]*ooking further to the* [complainant's] *account we have found that this player had only one account with us*". The controller further added that "*our support agents before sending any personal info they need to ensure that the request is legit. Technically there are always ways to false the senders email address and or a relative or friend get access to that email account. This happened a few times and fortunately because we follow our procedures we did not let this happen*".

10. On the same day, following the receipt of the above-mentioned email, the Commissioner requested the controller to provide additional clarifications to verify: (i) whether the procedure "*Managing Personal Data Requests*" submitted earlier on was adhered to, and (ii) whether it requested the complainant to confirm his e-mail address pursuant to the "*Template - GDPR Identity Verification*" and the "*Template - GDPR Identity confirmed*"[3]. The Commissioner also instructed the controller to submit copies of any documents where users were informed that a certified copy of their identity document may be requested by the controller as additional proof of identity.

11. On the same day, the controller replied that "*customer support agents are there to assist our clients* [...] *based on the user request and attitude we need to ensure that the person we are dealing on the other side is the actual person. As a company we prefer to follow our processes and even waste more recourses that we need just to ensure the security and privacy of our customers*".

12. By means of an email dated the 9th February 2021, the Commissioner reiterated his requests for the controller to provide evidence of adherence to the procedure "Managing Personal Data Requests" and to confirm that the complaint's e-mail address was requested pursuant to the "Template - GDPR Identity Verification" and to the "Template - GDPR Identity confirmed".

13. On the 10th February 2021, the controller further provided that "[t]*he verification procedure was followed by our agent. The player email address was validated and recorded as per internal process.* [...] *Personal data needs to be protected, and we had to ensure confidentiality, integrity and availability above all. Any data subject-access requests made by*

[3] The Commissioner received these documents from the controller during the course of the investigation of a separate case.

unauthorized persons will result in a breach. This is what we want to avoid in these type of cases". The controller also submitted a copy of their Privacy Policy and stressed that "[w]*e do not specify in our Privacy Policy the type of ID verification we require in order to process a GDPR request*".

LEGAL ANALYSIS AND DECISION

14. For the purpose of this legal analysis, the Commissioner sought in essence, to establish whether, by requesting the complainant a certified copy of his identity document prior to complying with his data subject's request submitted pursuant to article 15 of the Regulation, the controller has complied with its obligation to facilitate the exercise of data subject rights vis-à-vis article 12(2) of the Regulation.

15. By examining article 12(2) of the Regulation, the Commissioner has noted that such provision aims at ensuring that substantive rights of data subjects are safeguarded by establishing clear, proportionate and effective conditions as to how and when data subjects shall exercise their fundamental rights. The same article stipulates that "*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***" [emphasis has been added].

16. Furthermore, recital 64 of the Regulation states that the "*controller **should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers***[...]" [emphasis has been added].

17. Having noted that, although the Regulation does not prescribe how to authenticate a data subject, in one of its guidelines[4], the Article 29 Working Party ("**WP29**") has shed some light on the measures that a controller may adopt to verify the identity of the requesting party.
18. The WP29 elaborates that, where a data subject provides additional information enabling his or her identification, the controller shall not refuse to act on the request. Moreover, the WP29 articulates its position in the sense that "[i]*n essence, the ability for the data controller to request additional information to assess one's identity **cannot lead to excessive demands and***

[4] Article 29 Working Party, *Guidelines on the right to data portability*, 16/EN, WP 242 rev.01.

to the collection of personal data which are not relevant or necessary to strengthen the link between the individual and the personal data requested" [emphasis has been added].

19. Having further assessed that whilst the Regulation does not define the "***reasonable measures***" which may be used by the controller to verify the identity of the requesting person, recital 57 of the Regulation exemplifies a reasonable measure in the context of online services and online identifiers. In this regard, recital 57 states that verification may occur, "***for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller***" [emphasis has been added].

20. In this connection, the controller's request to verify the identity of the data subject shall be proportionate and, unless strictly necessary, the controller shall not require a broader range of personal data other than that which has already been processed prior to the request.

21. The Commissioner stresses that when the controller processes "***additional information***" for the purpose of identity verification, the controller shall ensure that such processing activity complies with the data minimisation principle pursuant to article 5(1)(c) of the Regulation. In this regard, the requested data shall be adequate, relevant and limited to what is necessary in relation to the purpose of the processing, in this case consisting in the identification of the data subject.

22. In this context, it is relevant to observe that the controller should take into account the broad range of categories of personal data included in a copy of an identity document and the risk arising from the processing of such personal data.

23. After examining the submissions, including the documents and clarifications provided by the controller, the Commissioner noted that the controller's procedure for ID verification does not dictate that a certified copy of the identity document is requested in every case, **but only in rare cases, where the customer support representative has doubts about the data subject's authenticity.** Additionally, such documents contain no references to requests concerning certified copies of identity documents for verification purposes upon receipt of a data subject request.

24. Initially, the controller explained that such doubts originated from the fact that the complainant had multiple accounts with the controller. However, at a later stage, the controller informed the Commissioner that the complainant had only one account.

25. Furthermore, the controller held that the request for a certified copy of an identity document following a data subject's request, was justified due to certain cases that the controller had previously suffered, whereby data subjects' requests were fraudulently submitted by third parties on behalf of, or acting as, the account holders. Nonetheless, the Commissioner assessed that such a fraudulent attempt has not occurred in the case under examination, given that the complainant's request was submitted by the same account holder.

26. In the present case, the Commissioner is of the view that the controller had no reason to have doubts concerning the complainant's identity, especially after the controller confirmed that the complainant had only one account. In any event, the controller could have used other reasonable measures to verify his identity, which means are as equally effective and efficient.

27. It therefore follows that the controller could have used measures which include *inter alia*, matching the information and personal data provided by the complainant with the identity document on file and, or requesting confirmation of further details, such as biographical details and details concerning the complainant's activity or usage of the controller's platforms.

28. As a consequence of the unjustified request for a certified copy of the complainant's identity card for identity verification purposes, the controller has not facilitated the exercise of the right of access by the complainant.

On the basis of the foregoing, the Commissioner hereby decides that the controller infringed article 12(2) of the Regulation for not having facilitated the exercise of the right of the complainant pursuant to article 15 of the Regulation.

In terms of article 58(2)(b) of the Regulation, the controller is hereby served with a reprimand and informed that in case of a similar infringement, the Commissioner shall take the appropriate corrective action, including an administrative fine.

In terms of article 58(2)(d) of the Regulation, the Commissioner is hereby ordering the controller to respond to the right of access request filed under article 15 of the Regulation by providing the complainant with a copy of his personal data undergoing processing by virtue of article 15(3) of the Regulation, as well as any other relevant information in terms of Article 15(1) thereof, letters (a) to (h).

The controller shall comply with the above order within five (5) days from the date of receipt of this legally binding-decision and inform the Commissioner immediately therafter.

In terms of article 83(6) of the Regulation, non-compliance with the aforesaid order shall "*be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher*".

By virtue of article 26(1) of the Data Protection Act (Cap. 586 of the Laws of Malta), any person to whom a legally binding decision of the Commissioner is addressed, shall have the right to appeal in writing to the Information and Data Protection Appeals Tribunal within twenty days from the service of the said decision as provided in article 23 thereof.

[redacted]

Information and Data Protection Commissioner

Decided today, the 4th **day of March, 2022**