Information and Data Protection Commissioner

CDP/IMI/LSA/4/2020

[redacted]

vs

[redacted]

COMPLAINT

1. On the 16th December. 2019, [redacted] (the **"complainant"**), residing in Germany, lodged a complaint with the supervisory authority of Germany against [redacted][1] (the **"controller"**) pursuant to article 77(1) of the General Data Protection Regulation[2] (the **"Regulation"**).

2. By virtue of article 56 of the Regulation, the supervisory authority of Germany identified Malta as the lead supervisory authority competent for the handling of the complaint. The Commissioner confirmed that it is indeed the lead supervisory authority and proceeded to investigate the complaint on the basis of the procedure set forth in article 60 of the Regulation.

3. The complainant submitted the following:

    a. that he learned through [redacted] that the controller had successfully carried out an identity verification check using his personal data, consisting of name, address, and date of birth;

[1] A company established in Malta, having its registered office [redacted] and bearing the registration number [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.

b. that he did not open an account with the controller or any other betting provider, and that this is a case of identity theft and misuse of data;

c. that accordingly, the complainant requested the controller to provide a copy of his stored personal data and delete or at least block his account, but the controller failed to do so.

INVESTIGATION

4. On the 18th December 2019, pursuant to article 58(1)(a) of the Regulation, the Commissioner requested the controller to provide its submissions in relation to the allegations raised by the complainant and any other information which it deems relevant and necessary.

5. On the 9th January 2020, the complainant submitted the following salient arguments for the Commissioner to consider in the legal analysis of the present case, including, an explanation on the registration and verification procedure carried out by [redacted]

Procedure for Registration and Identity Verification with the controller

a. that any person wishing to register an online account may do so by clicking on the "Register" button on the website, and following this, the person is prompted to input a number of details, which include the country, preferred username, email address, password, first name, last name, date of birth, nationality, country and city of birth, home address and mobile number;

b. that upon registration, the data subject is informed about the Terms and Conditions and the Privacy Policy, with the respective links to both being provided;

c. that Section VI of the Privacy Policy entitled the "Security, Identity Checks and Fraud Prevention" states that "[i]*f we are legally obliged or otherwise to check your identity, we reserve the right to protect our rightful interests by verifying your identity with the aid of, amongst other, the following companies:* [redacted] *(please note that we solely verify your identity with the help of* [redacted] *we do not carry out any credit checks; further information on* [redacted]

activities can be found online at [redacted] *Germany [...] To do so, we transfer the personal data provided to the above-listed companies, who will then run at appropriate check and verification. The information we receive from them will serve as a basis for our decision on whether to establish, conduct or terminate the contractual relationship*";

d. that the [redacted] identity verification checks are triggered upon a first deposit attempt, and the controller explained that, in the present case, a deposit attempt was made on the account following login, however, the deposit attempt was cancelled prior to it being completed, which automatically triggered a [redacted] identity verification request;

e. that upon receipt of the verification request [redacted] cross-checked the data received by the controller with its own database and returned a result to the controller, depending on whether the data are accurate or not;

f. that a data subject on whom a [redacted] check is carried out is made aware of any identity verification checks which are made through a statement they receive from [redacted] and in the case at hand, the data subject alleged that he discovered that an account had been opened in his name through this [redacted] statement;

g. that until a complete customer due diligence takes place on the account to verify the person's identity, the possibility that a person registers an account in the name of another is plausible;

Timeline & Facts of the Case

h. that the controller had its first contact with the complainant on the 14th April 2019[3], when the complainant wanted to know the reasons for the [redacted] request, and stated that he had not registered any accounts with the controller and therefore, requested more information about the data that the controller stored about him;

[3] A copy of the email sent by the complainant to the controller was attached with the submissions. The English version of the email dated the 14th April 2019, reads as follows: "*on March 26th, 2019 you made a request about me with the German* [redacted] *On what basis was this request made? I have no business relationship with you, nor have I ever been interested in it. In addition, tell me what data you have stored about me, where this data comes from, on what basis you have saved this data and with whom you have shared this data?*"

i. that the customer service team of the controller found an account with the name [redacted][4], however, besides the name, the controller had no further proof of the person's identity, and the email address from which the complainant contacted the controller was different to the one registered to the account, and the complainant failed to provide proof of the [redacted] check or any other information which could help the controller to verify the complainant's claims;

j. that accordingly, the controller immediately blocked the account due to suspicion of fraudulent activity, and the complainant's query was escalated internally by the Customer Service Agency in order to understand how best to proceed with this matter;

k. that once the controller carried out its verifications internally, it established that it does not have a sufficient legal basis to give the information to the requested party for the reasons outlined hereunder:

   i. that the controller was not convinced of the complainant's true identity, or rather, that the data on the account that was created with the controller truly all pertained to him;

   ii. that since there was an allegation of identity theft and the setting up of a fraudulent account, there was a high possibility of data commingling, possibly pertaining to the data subject himself, as well as the third party who opened the account in the data subject's name, or perhaps even to other third parties whose data such third party may have misappropriated. As an example, the controller explained that the third party may have used the data subject's name and date of birth, but at the same time used his own home address, email address and so on. Additionally, the controller stated that the IP address used to register the account would likely still not have been in a position to share this information with the complainant due to this uncertainty as to which data truly pertained to him, and which data pertained to the third party, or other third parties. It was therefore decided that providing the complainant with access to this data may

[4] A copy of the email sent by the controller to the complainant was attached with the submissions. The English version of the email dated the 17th April 2019, reads as follows: "*Due to very high volume, we apologize for the unusually long waiting time. An account was created with us under your data. The query at* [redacted] *is just an identity check and in no way an entry of something similar. As you say you have never used our service, this query was forwarded to our specialist department.*"

have resulted in the likelihood of a data breach and could have prejudiced potential (and now current) criminal investigations, leading to more serious consequences for the data subject, the controller and possibly other third parties.

l. that the controller proceeded to ask the allegedly aggrieved party to file a complaint with the police[5], and for the controller to cooperate directly with the Police on this matter upon request;

m. that on the 28th June 2019, the controller received an email from [redacted][6], requesting the controller to send her all the details of the fraudulent account, and according to the controller's internal procedures, any police requests the controller receive shall only be processed by the controller upon receipt of an official written request showing the police's official stamp[7];

n. that the controller further explained that the rationale behind its procedure is to ensure that it always provides information about their data subjects to an official verified source, due to the many fraudulent emails going around on the internet, even some claiming to be "official police requests", and for this reason, the controller requested [redacted], to submit a request showing the police's official stamp, and up until the date of the submissions, the controller did not receive any further correspondence or requests from the Police on this matter.

---

[5] A copy of the email sent by the controller to the complainant was attached with the submissions. The English version of the email dated the 22nd April 2019, reads as follows: "*Our specialist department has checked you request. An account has been created with us using your personal data. Since you are indicating that this was not you, we recommend reporting this to the police. We will make ourselves available to the authorities with all information at any time.*"

[6] A copy of the email sent by [redacted] to the controller was attached with the submissions. The English version of the email dated the 28th June 2019, reads as follows: "[a]*n investigation is being carried out for fraud, identity theft and suspected money laundering against unknown persons. The injured party* [redacted] *has filed a criminal complaint because an unlawful account was created using his personal data. You have denied the injured party further information and the deletion of his data by e-mail dated 22.04.2019 (your reference* [redacted]*. In order to continue the investigation, you will be asked to provide any information you have about the fraudulent account, as well as all transactions that were carried out via this account.*"

[7] A copy of the email sent by the controller to the Police was attached with the submissions. The English version of the email dated the 7th July 2019, reads as follows: "*We would be happy to help you clarify the situation. However, I would like to ask you to send the request for information in a scanned form (including the stamp) in response to this email. Of course, we will then be able to send you all this data available to us*".

6. After analysing the submissions and the communication attached therewith, the Commissioner noted that there was no correspondence which indicates that the controller had informed the complainant that the account linked to his name was blocked due to suspicion of fraudulent activity. In this regard, by means of an email dated the 11th March 2020, the controller was requested to indicate if the complainant was informed about this. On the 12th March 2020, the controller submitted evidence taken from its system, which demonstrates that the account pertaining to [redacted] was blocked on the 17th April 2019.

7. Additionally, during the course of the investigation, the Commissioner requested the controller to submit a copy of the email in the original language that it received from the Police on the 28th June 2019. Accordingly, the controller submitted a copy of the email, which was sent from this address: [redacted]

8. The Commissioner was further informed that, on the 18th October 2021, the Police requested the controller to provide all the information about the fraudulent account on the basis of the German Code of Criminal Procedure and the controller sent, to the Police, all the information about the fraudulent account file on the same day. Consequently, the Commissioner requested the German supervisory authority to provide any updates in relation to the Police investigations conducted by the German Police in relation to the alleged case of identity theft. On the 20th April 2022, the German supervisory authority informed the Commissioner that the case was dropped again at the end of 2021.

LEGAL ANALYSIS AND DECISION

9. On the 14th April 2019, the complainant exercised his right to access his personal data after he was informed that an identity verification check using his name, address, and date of birth, was successfully carried out by [redacted] the company that carries out appropriate checks and verifications on behalf of the controller. The controller informed the complainant that an account has been created using the complainant's personal data.

10. During the course of the investigation, it resulted that on the 17th April 2019, the controller had blocked the account linked to the name, [redacted] due to suspicion of fraudulent activity. This therefore means that the controller had restricted the processing activity in order to enable it to verify whether this was indeed a fraudulent activity. On the 24th September 2019, the complainant informed the controller that a criminal complaint has been filed with the Police

and provided the reference number of the case. Additionally, the complainant requested the controller to block his personal data until the investigation is completed.

11. From the investigation, it resulted that the complainant exercised his right of access pursuant to article 15 of the Regulation. The right of access enables the data subject to request the controller to provide access to his personal data, including information surrounding the processing activity. Article 15(1) of the Regulation states that the "*data subject shall have the right to obtain from the controller confirmation as to whether or* ***not personal data concerning him or her are being processed***" [emphasis has been added]. Pursuant to the Article 29 Working Party, information can be considered to relate to an individual when it is about the individual[8]. The opinion provides three alternative elements – content, purpose or result – to determine whether information "*relates to*" an individual. This has also been confirmed by the Court of Justice of the European Union, wherein it states that this element is fulfilled "*where the information, by reason of its content, purpose or effect, is linked to a particular person*"[9].

12. The Article 29 Working Party in its Guidelines[10] clarifies that "*personal data concerning the data subject*" shall not be interpreted in an overly restrictive manner by the controller. In this regard, the Guidelines provide that "[i]*n many circumstances, data controllers will process information that contains the personal data of several data subjects. Where this is the case, data controllers should not take an overly restrictive interpretation of the sentence "personal data concerning the data subject". As an example, telephone, interpersonal messaging or VoIP records may include (in the subscriber's account history) details of third parties involved in incoming and outgoing calls. Although records will therefore contain personal data concerning multiple people, subscribers should be able to have these records provided to them in response to data portability requests,* ***because the records are (also) concerning the data subject***." [emphasis has been added].

13. In its submissions, the controller stated that "[h]*ad we been convinced of the Data Subject's Identity, we would likely still not have been in a position to share this information with* [redacted] *directly due to this uncertainty as to which data truly pertained to him, and which data pertained to the third party, or other third parties*". During the course of the investigation, it

[8] Article 29 Working Party, Opinion 4/2007 on the concept of personal data.
[9] Case C-434/16, Peter Nowak vs Data Protection Commissioner, para. 35.
[10] Guidelines on the right to data portability, adopted on the 13th December 2016, as last revised and adopted on the 5th April 2017.

was established that the information stored by the controller is associated with or related to the identity of [redacted] and therefore this constitutes information which, by reason of its content, purpose or effect, is linked to [redacted]. It therefore follows that all personal data collected about the fraudster using the identity and personal data of [redacted] need to be disclosed to the complainant. This is without prejudice to the obligation of the controller to use all reasonable measures to verify the identity of the person making the request.

14. According to article 12(2) of the Regulation, the controller shall not refuse to act on the request of the data subject for exercising his rights, unless the controller demonstrates that it is not in a position to identify the data subject. In conjunction with this, article 12(6) of the Regulation puts an obligation upon the controller to verify the identity of the requesting party where the controller has reasonable doubts about the identity of the natural person. Whereas it is justified in such a situation at present for the controller to have reasonable doubts about the identity of the person making the request, however, the Commissioner is of the view that the controller should have requested the provision of additional information necessary to confirm the identity of the person exercising the right of access.

15. In its submissions, the controller provided that "*we received no proof of the* [redacted] *check from the Data Subject, and no further information which could help us verify his* [the complainant] *claims*". Pursuant to the accountability principle coupled with article 12(6) of the Regulation, it shall be the responsibility of the controller to demonstrate that it had requested the provision of additional information necessary to confirm the identity of the person making the subject access request. The Commissioner carefully examined the correspondence annexed to the submissions provided by the controller, wherein it is evident that the controller did not request the complainant to submit additional information to enable his identification, which identification check may include *inter alia*, a copy of the [redacted] check which the complainant received. It resulted that the controller only informed the complainant that a Police report should be lodged in relation to the matter.

16. Accordingly, the Police contacted the controller by means of an email dated the 28th June 2019, wherein the Police informed the controller that [redacted] had filed a criminal report and requested any information pertaining to the fraudulent account, as well as all transactions that were carried out via the account. During the course of the investigation, the controller submitted that at the time, the request submitted by [redacted] did not show the police's official stamp and therefore the request was not pursuant to its internal procedure. Within this context,

the Commissioner requested the controller to submit a copy of the email received from [redacted] in the German language. After assessing the copy of the email dated the 28th June 2019, particularly the email domain, the Commissioner determined that the email was legitimate, and the request was indeed coming from the Police.

17. At the time of the issuance of this legally-binding decision, the Commissioner had been informed that the police investigations were dropped and therefore, there is no evidence which concretely proves that this was a case of identity theft. However, the Commissioner clarifies that even if the Police had established that this indeed was a case of identity theft, the complainant shall have the right to be provided with information on all personal data the controller stored in connection with his identity, including, those that have been collected on the basis of the actions of the alleged fraudster.

On the basis of the foregoing considerations, the Commissioner decides that the controller infringed article 15(1) and 15(3) of the Regulation, when it failed to provide the complainant with a copy of his personal data undergoing processing and the information concerning the processing.

As a result, the controller is hereby being served with a reprimand pursuant to article 58(2)(b) of the Regulation and furthermore, in terms of article 58(2)(c) of the Regulation, the controller is hereby being ordered to comply with the subject access request submitted by the complainant, subject to the carrying out of the appropriate identity verification checks to confirm the identity of the complainant within ten (10) days from the date of receipt of this legally-binding decision. The controller shall provide proof of evidence to demonstrate compliance with the order of the Commissioner.

By virtue of article 83(6) of the Regulation, non-compliance with the order of the Commissioner shall, in accordance with article 58(2) thereof, be subject to an administrative fine 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.

[redacted]
(Signature)

Digitally signed by [redacted]
(Signature)
Date: 2023.09.05 13:04:50 +02'00'

[redacted]
Information and Data Protection Commissioner

Right of Appeal

The parties are hereby being informed that in terms 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 to the Information and Data Protection Appeals Tribunal within twenty (20) days from the service of the said decision as provided in article 23 thereof.

An appeal to the Tribunal shall be made in writing and addressed to "The Secretary, Information and Data Protection Appeals Tribunal, 158, Merchants Street, Valletta."