Information and Data Protection Commissioner

CDP/IMI/LSA/10/2020

[redacted]

vs

[redacted]

COMPLAINT

1. Reference is made to the complaint lodged by [redacted] (the "**complainant**" or the "**data subject**") on the 4th July 2019 against [redacted] (the "**controller**" or "[redacted]"), which has been referred to the Information and Data Protection Commissioner (the "**Commissioner**") by the Norwegian supervisory authority (the "**Datatilsynet**" or the "**Norwegian DPA**"), acting as the concerned supervisory authority.

2. The Norwegian DPA informed the Commissioner about the case on the 17th March 2020, when the Norwegian DPA initiated the procedure pursuant to article 56 of the General Data Protection Regulation[2] (the "**Regulation**"). Following an assessment carried out by the Commissioner, it was determined that the controller has its main establishment in Malta.

3. The complainant held an account with [redacted] and his complaint relates to the fact that the controller requested him to provide a copy of the bank's transaction history for the months of May and June 2019 as a way to sufficiently demonstrate that he has not received the [redacted]. The complainant considered this request to be excessive and unnecessary. Additionally, he complained about the lack of proper information in relation to who is the [redacted] provider, leading him to have no control over who has access to his personal data and how it is stored, managed and used.

[1] [redacted] is a private limited company registered under the laws of Malta with number [redacted] having its registered address at [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 (General Data Protection Regulation).

INVESTIGATION

4. 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. In terms of this Office's internal investigation procedure, the controller was provided with a copy of the complaint together with the supporting documents.

5. On the 2nd April 2020, the controller submitted the following principal legal arguments, together with supporting evidence[3], for the Commissioner to consider during the legal analysis of this case:

   a. that after the complainant was informed via an automated message that the [redacted] has been affected pursuant to its standard procedure, the complainant claimed that he did not receive his [redacted], a total sum of [redacted];

   b. that the customer support sent the complainant an excel file to prove that the [redacted] was processed, including a record of the date of w[redacted]l and the amount [redacted];

   c. that the complainant did not deem this to be sufficient and therefore, the controller had to find another way to verify if the complainant had received the [redacted] and accordingly, requested the customer to provide a bank statement, leaving the details relating to incoming transactions with an amount close to [redacted] visible, after the complainant objected to send his bank statements;

   d. that the controller requested the bank statements that would present the description of transactions for the following two (2) reasons: (i) the controller has a legitimate interest, particularly, to ensure with reasonable certainty that this is not a fraudulent claim; and (ii) the controller had previously encountered situations where customers were not recognising transactions due to a change in the billing descriptor and therefore, the controller wanted to verify whether this was also the issue in this particular case;

[3] Controller's confirmation of [redacted], Excel file with [redacted] history, complainant's bank account screenshots and original transcripts of communication between the controller and the complainant.

e. that the controller pointed out that the complainant provided only the information limited to dates and amounts [redacted], and therefore, at no time were full bank statements provided to the controller; and

f. that the controller outlined that it is the standard procedure to only request the minimum necessary information as required on ad hoc basis and in this specific case, due to issue which the controller was experiencing with [redacted] providers and potential change in the billing descriptor, the controller had determined that the most effective way to verify [redacted] was to request a bank statement from the complainant.

6. The Commissioner verified from the transcript of the communication exchanged between the controller and the complainant that the controller had sent the [redacted] reference number to the complainant. However the complainant was not able to find any [redacted] bearing this reference number when searching through the transactions of his bank account.

7. It also appears that on the 26th June 2019, the complainant copied and pasted a list containing some transactions as shown in his bank account and sent it to the controller by means of an email. The controller replied on the 27th June 2019 and provided the complainant with clearer instructions of what information was required to investigate the matter further: "*Please attach screenshots showing the full website, such as URL and the bank logo, including your bank account number and your full name. We would like the 2 last transactions on the first document that you submit to appear in the second document, so that the transactions overlap. Please note that we do not accept images of your transaction history from a cell phone. We prefer that you attach a PDF document reflecting your bank account".*

8. Following a request made by the Commissioner, by means of an email dated the 23rd July 2021, the controller explained that "*this specific [redacted] request did not trigger any identity verification procedures since, after assessing the customer request, operational teams did not identify flags that would require further verifications… the issue at hand was not the customer identity but whether the transaction was indeed conducted or not…the main issue, in this case, was whether the customer indeed received the [redacted] on her bank account. The customer had requested a [redacted], which was processed…However, despite all proofs of [redacted] provided by the customer support team, the customer claimed that the [redacted] had not been received. Such queries can happen as customers sometimes fail to identify [redacted], due to different descriptors used by*

payment service providers. However, ...since after all regular confirmations that were sent (OMS, transaction history, etc.), in this case, the customer was still not satisfied as she still claimed that the [redacted] *was not visible on her bank statements. Therefore, the only last resort to prove what factually happened was to request her bank statements to verify whether the transaction was received or not on her bank account".* The controller added that '[redacted] *believes that the request for such information is proportional in view that it is within legitimate interest to ensure that this is not a fraudulent claim, and also since from experience we are aware that certain payment providers can change billing descriptions."*

9. On the 27th July 2021, the controller confirmed that, even though it was not possible to make sure whether the [redacted] was received by the complainant given that the requested bank statement was never provided, the controller wanted to trust the complainant's good faith and decided to proceed with a new withdrawal[4] *"...but now via a different payment method. According to [the controller's] records, he got that payment*".

10. After the new [redacted] was processed, the controller never heard back from the complainant and presumed that the [redacted] was safely received and thus, the complainant was satisfied.

11. On the 29th October 2021, the Commissioner requested the controller to provide evidence of the issues encountered with some payment providers at the time when the complainant requested his [redacted] In its reply received on the 3rd November 2021, the controller provided evidence, in the form of a screen shot, "*showing execution of the transaction*" by the service provider. Moreover, the controller further explained that *"the payment provider successfully received the instruction for* [redacted]*, therefore, we did not see any issue that this customer might have had with the payment provider. However, since the customer was claiming that he did not get this payment, we thought that he might be having the same problem with identifying the billing descriptors, which other customers were reporting to us (customers were not seeing a proper description on their bank statement which clearly shows from where the funds were coming, as some payment service providers were using different descriptors)*".

12. The controller further added that *"[s]ince from our end we did, and to this date, do not have any proof that there was a problem with this transaction, but rather customer is the one*

[4] The controller '[redacted] *the funds to the customer account on 03.04.2020 and the customer* [redacted] *the funds on 25.06.2020*'.

claiming that he did not get the money from us in spite of all evidence provided from our end, our only last resort to prove what factually happened was to request his bank statement. This was necessary to verify whether the transaction was received or not on his bank account (by checking whether any date and amount matched the [redacted] *paid from our end, although the description might be different)".*

LEGAL ANALYSIS AND DECISION

13. For the purpose of this legal analysis, the Commissioner sought in essence, to establish the legal basis upon which the controller relied to request the complainant to provide a copy of his bank transaction history to verify if the [redacted] has indeed been received by the complainant and to determine whether the controller has fully complied with its information obligations pursuant to the requirements of the Regulation.

Lawful basis

14. In terms of article 8 of the Charter of Fundamental Rights of the European Union, personal data shall be processed fairly for specified purposes and on the basis of a legitimate basis laid down by law. In this respect, the Commissioner notes that the principle of lawful processing, which is one of the data protection principles, requires that every data processing operation has a lawful ground for processing. In this regard, article 6(1) of the Regulation stipulates what may constitute such a legal basis, taking also into consideration all the other core principles for processing personal data as set out in article 5 of the Regulation. Therefore, a controller shall be in a position to identify the appropriate legal basis before the processing activity, which corresponds to the objective and essence of the processing activity.

15. In his analysis, the Commissioner considered the submissions provided by the controller, wherein it argued that it is "*in our legitimate interest to ensure with reasonable certainty that this is not a fraudulent claim*" and therefore the request to provide a copy of the bank statement was based on article 6(1)(f) of the Regulation.

16. In this regard, the Commissioner assessed article 6(1)(f) of the Regulation, which states that the processing shall be lawful if it "*is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests*

or fundamental rights and freedoms of the data subject which require protection of personal data…".

17. Within this context, the Commissioner examined the judgments[5], delivered by the Court of Justice of the European Union (the "**Court**"), whereby it elaborated on the concept of the three-part test and stated that "*Article 7(f) of Directive 95/46 lays down **three cumulative conditions** so that the processing of personal data is lawful, namely, first, the **pursuit of a legitimate interest** by the data controller or by the third party or parties to whom the data are disclosed; second, **the need to process personal data** for the purposes of the legitimate interests pursued; and third, that **the fundamental rights and freedoms of the person concerned by the data protection do not take precedence**.*" [emphasis has been added].

18. Accordingly, the Commissioner assessed the present case in light of the three (3) cumulative conditions as laid down by the Court. All the three (3) conditions identified by the Court need to be present: (i) the existence of a legitimate interest justifying processing; (ii) the necessity of processing for the realisation of the legitimate interest; and (iii) the prevalence of that interest over the rights and interests of the data subject, which calls for balancing of interests.

19. First, the processing is conditional upon the existence of a legitimate interest of the controller or of a third party. The Regulation does not define legitimate interest and thus, it is for the controller to determine whether there is a legitimate aim that could justify an interference with the right to the protection of personal data.

20. The Commissioner interprets "*interest*" to be the broader stake that a controller may have in the processing, or the benefit that the controller or third parties may derive from such processing. This interpretation is substantiated by the recitals of the Regulation, which provide some non-exhaustive examples of situations in which legitimate interest could exist and this could be processing for the purpose of preventing fraud, processing for direct marketing purposes, the transmission of certain data within groups of companies and processing for the purpose of ensuring network and information security. Furthermore, the case-law of the Court of Justice of the European Union held that transparency or the protection of the property, health and family life are legitimate interests[6].

[5] Rigas satiksme, C-13/16, paragraph 28 and TK v Asociația de Proprietari bloc M5A-ScaraA, Case C-708/18, paragraph 40.
[6] Volker and Markus Schecke and Eifert, Case C-92/09 and C-93/09, paragraph 77 & Rynes, Case C-212/13, paragraph 34.

21. Pursuant to the Guidelines issued by the Article 29 Working Party[7], the interest is deemed to be 'legitimate' if it fulfills the following conditions: (i) it is lawful; (ii) it is sufficiently clearly and articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject; and (iii) represent a real and present interest.

22. The Article 29 Working Party recognises that *"prevention of fraud"* is one of the most common contexts in which the issue of legitimate interest may arise. Additionally, recital 47 of the Regulation provides that the *"processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned".* It therefore follows that the legitimate interest pursued by the controller is clearly articulated, effective and real, and consequently, justified.

23. In relation to the second condition, the Commissioner examined if the processing goes beyond what is necessary, and therefore assesses if the request made by the controller for a copy of the bank statements that would present a description of transactions, covering the period between the 23rd May 2019 until the 2nd July 2019, was necessary for the purpose of the attainment of the legitimate interest at issue.

24. The Commissioner notes that the principle of data minimisation as laid down in article 5(1)(c) of the Regulation requires that the processing shall be adequate, relevant and limited to what is necessary in relation to the purpose of the processing. It therefore follows that the processing of personal data shall be limited to what is plausibly necessary[8] to pursue a legitimate interest and therefore, there shall be a connection between the processing and the interest pursued. For this purpose, any data that is not directly linked to obtaining, realising or otherwise accomplishing the legitimate interests pursued is not lawfully processed.

25. Additionally, recital 39 of the Regulation sheds further light on the principle of data minimisation, by stipulating that "[p]*ersonal data should be processed only if the purpose of the processing* ***could not reasonably be fulfilled by other means***".

[7] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN WP 217, adopted on the 9th April 2014.
[8] Judgment of the European Court of Human Rights in the case Silver & Others v United Kingdom of 25 March 1983, para 97 discussing the term 'necessary in a democratic society': *"the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable"…."*

26. The Court of Justice of the European Union in its judgment 'TK vs Asociaţia de Proprietari bloc M5A-ScaraA'[9] states that the second condition relating to the principle of data minimisation "*requires the referring court to ascertain that the legitimate data processing interests pursued by the video surveillance at issue in the main proceedings — which consist, in essence, in ensuring the security of property and individuals and preventing crime — **cannot reasonably be as effectively achieved 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***." [emphasis has been added].

27. In this regard, the proportionality of the data processing should be assessed by taking into account the methods that could be used to effectively achieve the same results whilst limiting the effect on the rights and freedoms of the complainant. On that account, the Commissioner considers that the controller's approach to shift the burden of proof on the complainant and request him to provide a bank statement showing transactions over a period of time for the purpose of establishing whether a pay-out which they have made, and which they should be able to effectively demonstrate that it has been made, runs contrary to the principle of accountability. This consideration is being made while also taking into account the measures which the controller indeed has at its disposal to check or otherwise verify, internally, but also with other third party service providers with whom they have a contractual agreement involving processing activities of personal data, in this specific case, whether a pay-out to the data subject has been successfully affected or not.

28. After assessing the circumstances of the present case, the Commissioner noted that the request for all the transactions covering the period of over a month is deemed to be excessive as this inevitably leads to the further processing of personal data which are not relevant for attaining the objective of the controller.

29. Finally, article 6(1)(f) of the Regulation calls for a balancing test, which requires that the controller assesses whether the legitimate interest pursued by the third party is overridden by the interests or fundamental rights and freedoms of the complainant. In this respect, account shall be taken, *inter alia*, of the nature of the legitimate interest being pursued, the nature of the personal data at issue, and the impact on the data subject. In relation to the latter point, the

[9] Case C-708/18, 11h December 2019.

Article 29 Working Party[10] clarifies the purpose of article 6(1)(f) of the Regulation is not to prevent any negative impact on the data subject, but to prevent any disproportionate impact.

30. Pursuant to recital 47 of the Regulation, the existence of a legitimate interest needs a careful assessment, including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The Article 29 Working Party highlights that "*it is important to consider whether the status of the data controller, the nature of the relationship or the service provided, or the applicable legal or contractual obligations (or other promises made at the time of collection) could give rise to reasonable expectations of stricter confidentiality and stricter limitations on further use*".[11]

31. The recently adopted Guidelines[12] issued by the European Data Protection Board provide that the decisive criterion that should be taken into account by the controller is the intensity of the intervention that the processing poses for the rights and freedoms of the data subject. Within this context, the Commissioner examined the nature of the personal data requested by the controller, which would have led to the disclosure of all the complainant's banking transactions covering a period that exceeds more than one (1) month, in order to verify whether the complainant has indeed received a [redacted] of [redacted] From this data, certain inferences could be made in relation to the financial situation of the complainant, including information in relation to his income and spending habits or patterns. Therefore, after taking into account all the relevant factors which are balanced against the legitimate interest pursued by the controller, the Commissioner considers the significance of the complainant's fundamental right and determines that the balancing exercise tips in favour of the complainant.

Information Obligation

32. The complainant contended that the controller could potentially share the requested bank transactions with the supplier which the controller refused to identify, and therefore, the complainant alleged he has no control over who has access to his personal data, how his data are managed and stored, or utilised thereafter.

[10] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.
[11] Ibid. 9, page 40.
[12] Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, adopted on the 29th January 2020, para. 32.

33. Accordingly, the Commissioner proceeded to examine the privacy policy on the controller's website[13] available at the time of the complaint received by this Office to establish that the controller provided information to the data subjects in relation to the recipients to whom the controller might transfer or disclose the personal data at customer registration stage[14]. In fact, the Privacy Policy reads as follows: "*Your personal information may be transferred or disclosed (for the purposes described in this policy) to any company within the* [redacted] *and, subject to an appropriate agreement with third parties to process that personal information on our behalf, such as: Our* [redacted] *providers, based on your preferences, to process your* [redacted] *and* [redacted]".

34. Within this context, the Commissioner considered article 13(1)(e) of the Regulation, which provides that *"where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (e)* ***the recipients or categories of recipients of the personal data, if any****"* [emphasis has been added].

35. Thus, the Commissioner examined article 4(9) of the Regulation, which defines a *"recipient"* as *"a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not."* In this regard, the definition of "*recipient"* encompasses processors to whom personal data may be disclosed to, by the controller. The Article 29 Working Party Guidelines on Transparency under Regulation 2016/679[15] provide practical guidance and interpretative assistance on the requirements of article 13, which state the following: *"The actual (named) recipients of the personal data, or the categories of recipients, must be provided. In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients."*

[13] [redacted]

[14] The customer registration form on [redacted] includes a link to the Privacy Policy.

[15] Adopted on 29 November 2017 as last revised and adopted on 11 April 2018.

On the basis of the foregoing considerations, the Commissioner hereby decides that:

i. **by means of the privacy policy made available at registration stage, the controller has informed the complainant about the categories of recipients pursuant to the requirement set forth in article 13(1)(e) of the Regulation; and**

ii. **the request of the controller is deemed to be excessive and unnecessary for the purpose of attaining its legitimate interest, and therefore, not lawful pursuant to article 6(1) of the Regulation. Consequently, in terms of article 58(2)(b) of the Regulation, the Commissioner is hereby issuing a reprimand to the controller and warned that in the event of a similar infringement, he will take the appropriate corrective action in terms of his powers at law.**

In terms of article 78 of the Regulation, as further implemented under Part VII of the Data Protection Act (CAP. 586 of the laws of Malta), any party to this decision shall have the right to an effective judicial remedy by filing an appeal in writing before the Information and Data Protection Appeal Tribunal within 20 days from the service of this decision[16].

[redacted]
(Signature)

Digitally signed by [redacted]
Date: 2022.09.06 11:30:14 +02'00'

[16] More information about the Tribunal and the appeals procedure is accessible at https://idpc.org.mt/appeals-tribunal/