CDP/IMI/LSA/17/2020

Information and Data Protection Commissioner

[redacted]

vs

[redacted]

COMPLAINT

1. On the 28th May 2020, Mr [redacted] (the "**complainant**") filed a complaint (the "**complaint**") with the Spanish Agency for Data Protection (the "**Spanish SA**") against [redacted][1] (the "**controller**").

2. The complainant alleged that in October 2019, he had opened an account with the controller to carry out a few operations on the stock market, and that in December of the same year, he had requested the controller to close his account.

3. The complainant argued that, at the time of lodging the complaint, his account with the controller was still open, and he was still receiving messages from the controller. The complainant also contended that the controller had requested him to sign a copy of the agreement in order to close his account, due to the fact that such agreement had not been signed upon subscription.

4. Furthermore, the complainant maintained that, the day before the date of lodging the complaint, he had received a document from the controller's external auditor (the "**auditor**") wherein he was requested to confirm his balance at the end of the previous year and sign the document[2]. The complainant held that in such document, not only his personal data were

[1] [redacted]

[2] Infra, para. 11.

shown, but also those of other customers, including postal addresses, names, surnames and account balances.

5. From the analysis of the supporting evidence attached to the case, more specifically the thread of e-mails exchanged between the complainant and the controller, it transpires that on the 23rd February 2020, the complainant requested the controller to unsubscribe him from e-mail notifications and close his account.

6. On the 24th May 2020, the controller replied to the complainant indicating the procedure to unsubscribe from e-mail notifications. On the same day, the complainant informed the controller about his intention to close his account and that he did not manage to do that by following the suggested procedure.

7. On the 26th May 2020, the controller informed the complainant that "[w]*hen we checked our record we realized that you haven't signed the contract with* [redacted]. *Could you please access into your client portal by using below link and sign the agreement.* [redacted] *Note : you should already receive an another email about your portal password. Kindly check your email box*".

8. On the same day, the complainant replied to the controller and stressed that, in spite of the fact that he had sent many e-mails requesting the controller to remove him from its systems, he was still receiving e-mails. The controller replied that "[a]*fter you sign the agreement I will close your account and you won't receive any email no longer*".

9. On the 26th May 2020, the complainant rebutted that *"I don't need to sign anything. I've been with you since September last year, and now you're asking me for I-don't-know-what-agreement. Furthermore, a workmate of yours already contacted me to process the cancellation, and told me that it was done, what means that it was not so. As per GDPR, when I request the removal and the withdrawal of [...] access to my data, you have to process it without signing any agreement"*.

10. On the same day, the controller replied that "[…] *This agreement should have been signed at the beginning of account opening process but you haven't signed this agreement. First of all*

signing agreement is an obligation. It take five min signing then I will close your account and you will never receive any email from [redacted] *[…]".*

11. On the 27th May 2020, the auditor wrote to the complainant requesting him to confirm his portfolio holdings and cash balances held by the controller on his behalf. When providing such information, the auditor attached, not only a copy of the complainant's balances, but also those pertaining to third parties.

12. On the 17th June 2020, the Spanish SA informed the Information and Data Protection Commissioner (the "**Commissioner**") about the complaint by virtue of article 56 of the General Data Protection Regulation[3] (the **"Regulation"**). The Commissioner decided to handle the case pursuant to article 56 of the Regulation and informed the Spanish SA accordingly. As a consequence, the Commissioner handled the complaint in terms of article 60 of the Regulation.

INVESTIGATION

13. On the 17th June 2020, 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. In terms of this Office's internal investigation procedure, the controller was provided with a copy of the complaint, together with the supporting documents attached thereto.

14. On the 20th June 2020, the controller responded to the Commissioner's request, specifying that such submissions were about "*the complainant's right of erasure request exercised by the complainant by virtue of the withdrawal of his consent to* [redacted]*'s access to the Personal Data*". The controller presented the following principal legal arguments for the Commissioner to take into consideration during the legal analysis of the case:

    i. that "[redacted] *is a company which performs investment services in accordance with its license as issued by the Malta Financial Services Authority (hereinafter referred to*

[3] 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).

as the "MFSA") under the Investment Services Act [Chapter 370 of the Laws of Malta] (hereinafter referred to as the "Act"). Accordingly, [redacted] *is subject to a variety of obligations, including strict anti-money laundering and compliance related obligations, arising from, inter alia, the Act, subsidiary legislation as emanating therefrom, the Investment Services Rules for Investment Services Providers as issued by the MFSA, the Conduct of Business Rulebook which is likewise issued by the MFSA, the Prevention of Money Laundering Act [Chapter 373 of the Laws of Malta], the Prevention of Money Laundering and Funding of Terrorism Regulations [Subsidiary Legislation 373.01] and the Implementing Procedures issued by the Financial Intelligence Analysis Unit in terms of the provisions of the Prevention of Money Laundering and Funding of Terrorism Regulations [S.L 373.01]. Furthermore,* [redacted] *is also regulated by numerous European regulations and directives*".

ii. that "[o]*ne such obligation to which* [redacted] *is subject is a yearly statutory audit conducted by an independent third party. This is a legal obligation to which* [redacted] *is subject and the processing of the Personal Data is necessary for compliance with such legal obligation*";

iii. that "[t]*herefore, whilst it is appreciated that any data subject may exercise the right to erasure of personal data in terms of Article 17(1) of the GDPR, Article 17(3) thereof provides exceptions to this right. Of relevance is Article 17(3)(b) which states that the right to erasure as set out in Article 17(1) of the GDPR shall not apply to the extent that processing thereof is necessary "for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*";

iv. that "[a]*ccordingly,* [redacted] *did not fully erase the Personal Data by virtue of the fact that the processing thereof is required in order to comply with a legal obligation to which it is subject in accordance with Article 17(3)(b) of the GDPR*";

v. that "[redacted] *respectfully submits that despite the complainant's request for erasure of the Personal Data, it had, and still has, every right and indeed, a legal obligation, to process the Personal Data in accordance with the provisions of the GDPR";*

vi. that "[…] *the retention (for a certain time period) of such Personal Data forming the subject matter of the Complaint by* [redacted] *is further necessary in order for* [redacted] *to comply with its anti-money laundering obligations";*

vii. that in relation to the fact that the controller requested the complainant to sign an agreement, the controller provided that the agreement *"was never signed at the beginning of the relationship between the complainant and* [redacted] […] *is necessary in satisfaction of* [redacted]*'s legal obligations with respect to client onboarding procedures. The complainant was requested to sign this agreement prior to the opening of his trading account with* [redacted] *and has no relevance to his request for the erasure of the Personal Data";* and

viii. additionally, the controller contended that *"without prejudice to the foregoing, it is recognized that in order for a controller of personal data to be obliged to delete personal data of a data subject following a request for such erasure in terms of the provisions of the GDPR, one of the grounds as set out in Article 17(1) thereof must apply, which is not the case in the matter at hand".*

15. On the 3rd September 2021, the Commissioner requested the following additional information from the controller:

i. the legal basis for processing the complainant's personal data;

ii. in the event that such legal basis is consent, evidence that the complainant has given consent for the processing of his personal data at the time when the business relationship commenced; and

iii. a copy of the controller's policy/procedure related to the handling of the data subjects' requests.

16. On the 7th September 2021, the controller submitted that "*the processing of the Claimant's personal data was therefore necessary for compliance with various legal obligations to which* [redacted] *is subject in accordance with Article 6(1)(c)*". In support of its arguments, the controller attached a copy of its privacy policy, which copy was delivered to the complainant.

17. On the 9th September 2021, the Commissioner requested the controller to submit a copy of the controller's policy/procedure related to data subject's right of erasure requests, which the controller did not submit with its previous response.

18. On the 13th September 2021, the controller submitted a copy of its "Operations Department Manual Procedure" and of its "Compliance Manual". The Commissioner noted that the procedure for handling the right of erasure requests was included in the first of the two documents.

19. On the 30th November 2021, the Commissioner requested the controller to provide any evidence to prove that the complainant's account was closed as requested by the complainant on the 23rd February 2020.

20. On the 30th November 2021, the controller confirmed that the last e-mail that was sent to the complainant was on the 26th May 2020. The controller reiterated that they "*explained him why we need this contract but he insisted to reject to sign the Contract and we Closed his account as of 26.05.2020 operations Department did not send another e-mail to the Client related with Account Closure*". On the same day, as attachment to another email, the controller also provided "the screenshots of account closure".

LEGAL ANALYSIS AND DECISION

21. As part of the investigation of this complaint, the Commissioner examined the part of the complaint, wherein the complainant contended that he had received a document, which contains the personal data of third parties. In terms of article 77(1) of the Regulation, a complaint may only be lodged with a supervisory authority if the data subject considers that the processing of personal data relating to him or her infringes the provisions of the Regulation. It therefore follows that the complainant was not one of the affected data subjects, and therefore, for the purposes of this legal analysis, this part of the complaint is being

dismissed. Having said this, the Commissioner reserve the right to start a separe investigation on the alleged personal data breach committed by the controller's auditor.

22. In this regard, in terms of article 57(1)(f) of the Regulation, the Commissioner proceeded to examine, to the extent appropriate, the subject-matter of the complaint, specifically : (i) the complainant's request to exercise his right to erasure; and the (ii) timing of the request.

The complainant's request to exercise the right to erasure

23. Having noted that the protection of natural persons in relation to the processing of their personal data is a fundamental right recognised by article 8(1) of the Charter of Fundamental Rights of the European Union[4]. Within this context, the rights of the data subjects as laid down in articles 12 to 22 of the Regulation are the fulcrum and the basis of the law, and their role is crucial to ensure the effective and comprehensive protection of their personal data processed by controllers.

24. Having examined the right to erasure as laid down in article 17 of the Regulation, according to which the data subject shall have the right to obtain from the controller erasure of his personal data and the controller shall have the obligation to erase personal data without undue delay. The exercise of the right to erasure is subject to the applicability of one of the legal grounds listed in paragraph 1 thereof.

25. Having noted that, by way of exemption from the general rule, article 17(3) of the Regulation, which prescribes that paragraphs 1 and 2 shall not apply insofar as the processing is necessary for certain, specific purposes or compelling requirements, as exhaustively provided therein.

26. Having given due regard to the fact that, in this respect, article 17(3)(b) of the Regulation excludes the applicability of the right to erasure to the extent that processing is necessary for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

[4] Charter of Fundamental Rights of The European Union, 2012/C 326/02.

27. Having examined the controller's submissions, wherein the latter declared that it was subject to legal obligations mandating that certain customer records – which include personal data – are retained for a stipulated period of time[5]. In this respect, the controller declared that "*the retention (for a certain time period) of such Personal Data forming the subject matter of the Complaint by* [redacted] *is further necessary in order for* [redacted] *to comply with its anti-money laundering obligations*".

28. Having observed that for the purpose of the Prevention of Money Laundering and Funding of Terrorism Regulations, Subsidiary Legislation 373.01, the controller is deemed to be a subject person. Article 13(2) of S.L. 373.01 stipulates that certain documentation, data or information as referred to in sub-regulation 1 thereof, shall be retained for a period of five (5) years commencing from the triggering events prescribed therein.

29. Having further determined that indeed, processing of customers' records by the controller is necessary for compliance with the aforesaid provision, to which the controller is subject.

30. Having considered that, as declared by the controller[6], the complainant's account has been closed on the 26th May 2020, and thus, the five-year period prescribed by the aforesaid provision had not elapsed at the time when the complainant lodged his complaint in terms of article 77(1) of the Regulation.

31. In view of the foregoing, the Commissioner concludes that, at the time when the complaint was lodged, the grounds listed in article 17(1) of the Regulation did not apply to the extent that processing is necessary for compliance with a legal obligation to which the controller is subject, and which requires processing by virtue of regulation 13(2) of S.L. 373.01.

<u>The timing of the request</u>

32. Having examined article 12 of the Regulation, which establishes clear, proportionate and effective conditions as to how and when data subjects shall exercise their rights provided by the Regulation.

[5] Supra, para. 14(1).
[6] Supra, para. 20.

33. Having noted paragraph 3 thereof, which aims at ensuring the efficient and timely exercise of data subjects' rights binding the controller to *"provide information on action taken on a request under Articles 15 to 22 to the data subject* ***without undue delay and in any event within one month of receipt of the request****"* [emphasis has been added].

34. Having considered that on the 23rd February 2020, the complainant requested the controller to exercise his right to erasure pursuant to article 17 of the Regulation and that in response, the controller requested the complainant to sign and return the subscription agreement. In addition, the controller informed the complainant on how to unsubscribe from receiving e-mail notifications.

35. In the correspondence exchanged between the controller and the complainant, the Commissioner could observe that the controller failed to inform the complainant about the steps taken in relation to the right to erasure request, and instead requested the complainant to sign and return the subscription agreement. The Commissioner emphasises that any failure on the controller's part to fulfil its own procedural or legal obligations, in this specifc case to ensure that the complainant signs the subscription agreement, shall be independent of, and certainly shall not have an impact on, the exercise of the complainant's data protection rights.

36. Having further examined that the controller's procedure[7] concerning the right of erasure requests, included in the "*Operations Department Manual*" submitted to this Office, wherein it resulted that the controller did not follow such procedure whilst handling the right to erasure request exercised by the complainant.

37. Having considered the Guidelines issued by the Article 29 Working Party, which provide that "[…]***failure to read and abide by existing policies****, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them)* ***may be indicative of negligence***"[8]

---

[7] "[t]*he controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request.* […] *If the request of the Client is related with erasure of Personal Identification Document(s),* [redacted] ***informs the Client that his request is not possible as per related rules and regulations and said documents will be kept at least 5 years in our records*** […]" [emphasis has been added].

[8] Article 29 Data Protection Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, 17/EN WP 253, page 12.

[emphasis has been added]. In this regard, the Commissioner established that, despite the fact that the controller had in place a policy in relation to the handling of the right to erasure requests, however, it failed to comply with its own procedure, which is an indicator of the fact that the controller acted negligently when the request submitted by the complainant was not handled in a timely manner, as prescribed in article 12(3) of the Regulation.

On the basis of the foregoing, the Commissioner hereby decides that the controller infringed article 12(3) of the Regulation, when it failed to provide the complainant with information on the action taken in relation to his right to erasure request submitted on the 23rd February 2020, within one (1) month of receipt of such request.

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

In terms of article 58(2)(d) of the Regulation, the controller is hereby being ordered to provide the complainant with a reply to his right of erasure request and his request to close his account. This order shall be implemented with ten (10) days from the date of receipt of this legally-binding decision and the controller is requested to inform the Commissioner with the action taken to comply with such order immediately thereafter.

The controller is additionally being reminded that, by virtue of article 12(1) of the Regulation, the reply to the complainant shall be provided in a concise, transparent, intelligible and easily accessible form, using clear an plain language, in particular by including information relating to the specific legislation which obliges the controller to comply with the requirements deriving therefrom and retain personal data for the prescribe timeframe.

[redacted]

Information and Data Protection Commissioner

Decided today, the 28th **day of February, 2022**