Information and Data Protection Commissioner

CDP/COMP/332/2024

[redacted]

vs

[redacted]

COMPLAINT

1. On the 22nd July 2024, [redacted] (the "**complainant**") lodged a complaint with the Information and Data Protection Commissioner (the "**Commissioner**") pursuant to article 77(1) of the General Data Protection Regulation[1] (the "**Regulation**"), alleging that [redacted]. (the "**controller**") failed to handle his request to access all his personal data pursuant to the requirements of the Regulation, and as a result, the controller infringed the provisions of the Regulation.

2. The complainant contended that he sought full access to all his personal data held by the controller concerning himself, including internal emails exchanged among employees and any other documents or briefs written about him, particularly those related to case [redacted] and his transaction on the 1st September 2023, within the date range of the 1st June 2023 to the 3rd June 2024.

3. The complainant submitted the following timeline in relation to the exercise of his right of access in terms of article 15 of the Regulation:

3rd June 2024	The complainant submitted a formal subject access request to access all his personal data and correspondence in relation to him.
28th June 2024	The controller provided partial documentation, including the Customer Due Diligence Form, details of customer and accounts,

[1] 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).

	statements of active accounts, and correspondence between the complainant and bank officials. The controller claimed that no information was shared with third parties.
1st July 2024	The complainant reiterated his request for internal emails and documents related to [redacted] as the initial response of the controller was incomplete.
5th July 2024	The controller stated that all the personal data pertaining to the complainant have already been provided, but refused to share internal communications, citing article 15(4) of the Regulation and professional and bank secrecy.
10th July 2024	The complainant clarified that his request pertains specifically to his personal data and not to third-party data, emphasising that the bank secrecy law should not prevent the complainant from accessing his own personal data.
16th July 2024	The controller reaffirmed that no additional personal data concerning the complainant exist beyond what have already been provided, contradicting its earlier acknowledgment of internal emails and other correspondence.
19th July 2024	The controller confirmed that its response dated the 16th July 2024 was its final reply in relation to the matter.

4. The complainant referred to the replies of the controller and alleged that these reveal several contradictory and conflicting replies regarding his request to access his personal data. On the 5th July 2024, the controller acknowledged the existence of internal emails and other correspondence in relation to the complainant, but refused to provide access to this documentation, citing article 15(4) of the Regulation, and professional and bank secrecy. However, in the subsequent response dated the 16th July 2024, the controller stated that it did not possess any additional personal data pertaining to the complainant beyond what have already been provided. The complainant contended that these conflicting statements indicate lack of transparency and compliance with his subject access request.

5. The complainant submitted that he has the right to access all his personal data, and this includes internal communications and documents that relate to his transactions and interactions with the bank pursuant to article 15 of the Regulation. The refusal of the bank, under the guise of bank secrecy, is not justified as these laws in relation to professional and bank secrecy are designed to protect clients from third-party disclosure, and not to withhold information from the data subjects themselves.

INVESTIGATION

6. Pursuant to the internal investigative procedure of this Office, the Commissioner provided the controller with a copy of the complaint, including the supporting documentation, and enabled the controller to submit any information which it deemed relevant and necessary to defend itself against the allegation raised by the complainant.

Submissions of the controller

7. By means of a letter dated the 10th September 2024, the controller submitted the following salient arguments for the Commissioner to consider during the legal analysis of this case:

   a. that the controller received a request via email from the complainant on the 3rd June 2024, requesting access to all data and correspondence pertaining to him, specifically the following information:

      - "*All personal data, transaction records, communication logs, and any other relevant information held by the Bank for the period 1st June 2023 to 3rd June 2024;*
      - *Information shared with third parties during this specified period, including but not limited to other financial institutions and intermediaries outside of the Bank; and*
      - *Copies of all documents and data written about him*";

   b. that following an internal analysis, in line with the Regulation and the controller's internal guidelines, on the 28th June 2024, the data protection officer provided the following list of documents held by the controller pertaining to the personal data of the complainant:

- *"Copy of the Customer Due Diligence Form as at 25th June 2024, including all information gathered from [redacted] as per KYC and other legal obligations.*
- *Copy of the Details of Customer and Accounts as at 25th June 2024, held in the Bank's systems.*
- *Statement of 3 active bank accounts held in the name of [redacted] from the period of 1st June 2023 to 3rd June 2024.*
- *Copy of the Office of the Arbiter for Financial Services ("OAFS") Case Ref: [redacted], which included record of the case filed before the Arbiter and all correspondence between [redacted] and Bank officials.";*

c. that further to the above, the controller informed the complainant that his personal data were not shared with other third parties other than the Office of the Arbiter for Financial Services;

d. that following the correspondence of the 28th June 2024, the complainant indicated that he did not receive all the data that he requested, and this is because copies of internal emails and documents containing his personal data were not provided, with specific reference to the Arbiter case;

e. that the complainant also requested access to reports, notes, any other communications created by the controller's officials and any other internal departments or personnel, within the period of the 1st June 2023 and the 3rd June 2024;

f. that the controller informed the complainant that all personal data held on his behalf were provided in good order following his first request, and therefore, the controller is of the opinion that internal communication is the sole property of the controller and cannot be shared with third parties, due to the fact that as per article 15(4) of the Regulation, this may adversely affect the rights and freedoms of others, particularly bank officials, who are bound with professional and bank secrecy;

g. that, in the reply, the controller further assured the complainant that notwithstanding the foregoing, no personal data concerning him, other than that already shared in his first reply was processed in the handling of the [redacted] and

h. that the controller has honoured the complainant's right of access to his personal data in line with article 15 of the Regulation and has provided all the relevant data.

8. By means of an email dated the 12th September 2024, the Commissioner ordered the controller to provide him with a copy of the internal communications which according to the controller "*may adversely affect the rights and freedoms of others, particularly Bank Officials, who are bound with professional and bank secrecy*". Furthermore, the Commissioner requested the controller to further substantiate the reasoning that led to the imposition of a limitation pursuant to article 15(4) of the Regulation and to clearly outline who may be adversely affected and how.

9. On the 17th September 2024, the controller submitted "*copies of the internal correspondence shared via electronic mail between* [redacted] *Bank employees regarding the formal OAFS complaint* [redacted]". The controller submitted that "[a]*s may be noted from the attached, several Bank employees were involved in the investigation ... Given that internal affairs such as the Bank's internally issued circulars and customer acceptance policy were being discussed, without any reference to specific personal data whatsoever, we reiterate our position that the Bank as the Data Controller did not have any obligation to share this particularly internal correspondence with the complainant. Additionally details of Bank Officials such as their name, work email addresses, designations and roles are also disclosed and accessible through such correspondence*".

Submissions of the complainant

10. As part of the internal investigative procedure of this Office, the complainant was provided with a copy of the controller's submissions and the opportunity to submit his counterarguments. By means of an email dated the 18th September 2024, the complainant submitted the following principal arguments for the Commissioner to consider during the legal analysis of this complaint:

    a. that the controller incorrectly refers to the complainant as a third party when it stated that "*internal communication is the sole property of* [redacted] *and cannot be shared with third parties*", and this misclassification indicates a fundamental misunderstanding of the Regulation, particularly, the controller undermines the right of the complainant as a data subject who is seeking access to his personal data, regardless of where his personal data are stored within the organisation;

    b. that article 15(4) of the Regulation must be applied narrowly and requires specific justification, and the controller has not specified which rights and freedoms of others would be adversely affected, nor provided a detailed explanation of how disclosure

would harm these rights, and general references to professional and bank secrecy are insufficient under the Regulation to deny a data subject access to his personal data;

c. that the controller asserted that internal communications are "*the sole property of* [redacted] *Bank plc and cannot be shared with third parties*", however, personal data is defined as any information relating to an identified or identifiable natural person, and therefore, the personal data pertaining to the complainant cannot be considered as proprietary in a manner that overrides his rights as a data subject;

d. that while the controller may own the medium (e.g., internal emails), this does not negate its obligation to provide access to personal data contained in those communications, and claims of ownership cannot be used to circumvent the obligations of the Regulation;

e. that as a matter of professional scepticism, the complainant does not assume that the controller had shared his data with unauthorised third parties, however, given the inconsistencies in the statements of the controller, the complainant prefers to verify rather than simply trust;

f. that, in the email dated the 5th July 2024, the controller admitted possessing emails and other correspondence about the complainant, but refused to provide them, however, in its email dated the 16th July 2024, the controller stated that no additional personal data exist, and therefore, this inconsistency raises questions about the thoroughness of the responses of the controller;

g. that the controller has not provided all personal data processed concerning the complainant, specifically internal communications related to his case [redacted] and his transaction of the 1st September 2023, and additionally, the controller did not adequately explain the reasons for withholding the data;

h. that by not conducting a thorough search across all systems and failing to provide a complete response, the controller has not facilitated the exercise of the complainant's rights under the Regulation, and the responses of the controller lack the clarity and completeness required by the Regulation, impeding the complainant's ability to understand and verify the processing of his personal data;

i. that the controller's lack of clear communication and failure to provide specific reasons for withholding the data undermine transparency and without adequate justification, the controller failed to demonstrate accountability for its data processing activities, and therefore, this is an infringement of article 5(1)(a) and article 5(2) of the Regulation;

j. that by withholding the personal data of the complainant without a valid justification, the controller disrupts the principle of purpose limitation, and the controller failed to demonstrate that withholding the data is necessary or aligned with the original purposes of the processing: and

k. that by not disclosing internal communications containing the complainant's personal data, the controller prevents the complainant from fully understanding how the data are used, and this hinders the complainant his ability to verify the lawfulness and accuracy of the processing to exercise his right to rectification, or erasure, and to understand the rationale behind decisions affecting him.

Final submissions of the controller

11. The controller was provided with the final opportunity to rebut the arguments made by the complainant. On the 20th September 2024, the controller submitted that:

> *"As data controllers we have honoured the complainant's right of access at first hand by providing all personal data held by the Bank. The additional internal correspondence was shared with your office for investigatory purposes, and as one might notice there is no personal data other than that already shared with the complainant processed through such electronic mail, hence there has been no personal data withheld by the Bank. The purpose of these correspondence exchanges was purely to investigate and coordinate the complainant request then made to the OAFS, from an internal governance perspective."*

Clarification

12. In addition, by means of an email dated the 23rd September 2024, the Commissioner requested the controller to indicate if the information in relation to the processing activity pursuant to article 15(1)(a) to (h) was provided to the complainant.

13. On the 27th September 2024, the controller submitted that "*copies of the personal data held by the Bank on behalf of the complainant which is processed for the purposes of maintaining the banking relationship has been provided to the complainant. Furthermore, the complainant had acknowledged and consented to the Bank's Data Privacy Policy, all of such pursuant to article 15(1)(a) to (h) of the GDPR*".

LEGAL ANALYSIS AND DECISION

The Subject Access Request

14. As a preliminary step of the investigation, the Commissioner sought to examine the request made by the complainant, wherein he requested the controller to provide access to his personal data pursuant to article 15 of the Regulation. By means of an email dated the 3rd June 2024, the complainant exercised his right of access and requested the controller to provide the following information:

> "*Pursuant to the General Data Protection Regulation (GDPR), I am writing to formally request access to all data and correspondence pertaining to myself,* [redacted] *identified by ID Card number* [redacted]. *Specifically, I am requesting the following information:*
>
> *1. All personal data, transaction records, communication logs, and any other relevant information held by your bank from the period of 1st June 2023 to 3rd June 2024.*
>
> *2. Information shared with third parties during this specified period, including but not limited to other financial institutions and intermediaries outside of* [redacted]
>
> *3. Copies of all documents and data written about me.*"

15. On the 28th June 2024, the controller replied to the request of the complainant by providing the following information:

> "*Please find attached all Bank documents which include your personal information as listed below:*

Copy of the Customer Due Diligence Form as at 25th June 2024.

Copy of the Details of Customer and Accounts as at 25th June 2024.

Statement of 3 active accounts from the period of 1st June 2023 to 3rd June 2024.

[redacted]. *This also includes all correspondence between yourself and Bank officials.*

With regards to "Information shared with third parties during this specified period, including but not limited to other financial institutions and intermediaries outside of [redacted]*", kindly note that no information was shared with third parties".*

16. On the 1st July 2024, the complainant argued that the information which was provided by the controller was incomplete and requested the controller to provide "*copies of all internal emails and documents related to case* [redacted] *including but not limited to reports, notes, and other communications created by* [redacted] *and any other internal departments or personnel, within the period of 1st June 2023 to 3rd June 2024*".

17. On the 5th July 2024, the controller replied that:

"*With reference to your request for copies of all internal emails and documents related to case* [redacted] *including but not limited to reports, notes, and, emails, kindly note that all personal data that the Bank has on your good self has been provided in our previous correspondence.*

Please note that internal communication is the sole property of [redacted] *plc and cannot be shared with third parties, due to the fact that as per Article 15(4) of the GDPR this may adversely affect the rights and freedoms of others, particularly Bank officials, who are bound with professional and bank secrecy.*

Conclusively, we would like to assure you that no personal data concerning your kind self, other than that already shared with you as part of PDF file [redacted] *which have been provided by your true self for management of the banking relationship with* [redacted] *was processed in the handling of case* [redacted]".

18. For the purpose of the investigation of this data protection complaint, the Commissioner sought to establish, in essence, whether: (i) the controller handled the request of the complainant pursuant to the requirements of the Regulation, read in the light of the transparency obligations; and (ii) the limitation invoked by the controller pursuant to article 15(4) of the Regulation was justified.

The Handling of the Subject Access Request

19. The right of access is a fundamental right of the data subject, and the law has designed a specific mechanism to easily enable the data subject to obtain from the controller information in relation to the processing activity pursuant to article 15(1)(a) to (h) of the Regulation, and where applicable, article 15(2) of the Regulation, and access to a copy of the personal data undergoing processing in accordance with article 15(3) of the Regulation.

20. The Commissioner noted that the request of the complainant was for "*access to **all** data and correspondence pertaining to myself* [the complainant]" [emphasis has been added]. However, this request was limited to all the personal data which were processed by the controller during the timeframe specified by the complainant in his request, that is, from the 1st June 2023 to the 3rd June 2024. Therefore, in such case, the request of the complainant is understood to encompass all the personal data pertaining to him, which were processed by the controller during the timeframe specified in the subject access request dated the 3rd June 2024.

21. In the reply dated the 28th June 2024, the controller informed the complainant that "***all** Bank documents which include your personal information*" were being provided [emphasis has been added]. However, following further questioning by the complainant, the controller informed the complainant on the 5th July 2024 that "***internal communication is the sole property of [redacted] and cannot be shared with third parties, due to the fact that as per Article 15(4) of the GDPR this may adversely affect the rights and freedoms of others, particularly Bank officials, who are bound with professional and bank secrecy***" [emphasis has been added].

22. After examining the exchange of correspondence between the parties, the Commissioner noted that the first reply of the controller dated the 28th June 2024 confirmed to the complainant that all the bank documents which contained his personal data were provided. Following further inquiry by the complainant, the controller informed the complainant that internal communications exchanged among the employees is the sole property of the controller, and therefore, on the basis of article 15(4) of the Regulation, this information was being limited.

Despite the fact that the controller invoked article 15(4) of the Regulation, it still insisted that "*all personal data that the Bank has on your good self has been provided in our previous correspondence*". This statement is self-contradictory because the controller cannot claim to have provided all the personal data pertaining to the complainant while simultaneously limiting the complainant's right of access to his personal data contained in the internal communications exchanged among its employees as per article 15(4) of the Regulation.

23. The principles of fairness and transparency as set forth in article 5(1)(a) of the Regulation extend to the exercise of the rights of the data subjects, including the replies provided by controllers concerning information and access to personal data pertaining to data subjects. The European Data Protection Board (the "**EDPB**") in its 'Guidelines 01/2022 on data subject rights – Right of access'[2] (the "**EDPB Guidelines**") states that the data subjects should be informed that the right of access is not only being limited in terms of article 15(4) of the Regulation, but also of the reason of such limitation. This is necessary to enable the data subjects to understand the action taken by the controller in relation to their personal data and challenge the decision of the controller in an effective manner using the appropriate remedies provided by the Regulation and the Data Protection Act (Cap. 586 of the Laws of Malta). For this reason, the EDPB states that:

> "*If controllers refuse to act on a request for the right of access in whole or in part under Art. 15(4) GDPR,* ***they have to inform the data subject of the reasons*** *without delay and at the latest within one month (Art. 12(4) GDPR). The explanatory statement has to refer to the concrete circumstances in order to allow the data subjects to assess whether they want to take action against the refusal. It must include information about the possibility of lodging a complaint with a supervisory authority (Art. 77 GDPR) and seeking judicial remedy (Art. 79 GDPR).*"[3] [emphasis has been added]

24. In his considerations, the Commissioner noted that the first reply of the controller failed to mention that the right of access was being partially limited in terms of article 15(4) of the Regulation. This led the Commissioner to conclude that the controller failed to inform the complainant about the imposition of a limitation in relation to his personal data contained in the internal correspondence of the bank, and therefore, the reply lacked the necessary elements of transparency and fairness. It was only after the complainant inquired further that he received a reply from the controller that his right was being partially limited in terms of article 15(4) of the

[2] Version 2.1, adopted on the 28th March 2023.
[3] ibid 2, paragraph 174.

Regulation. If the complainant had not sought further clarifications from the controller, he would have remained unaware of the partial limitation imposed by the controller.

Information in relation to the processing as set forth in article 15(1)(a) to (h) of the Regulation.

25. During the course of the investigation, the Commissioner requested the controller to clarify whether the complainant was provided with information in relation to the processing as required by article 15(1)(a) to (h) of the Regulation. The controller submitted that "*the complainant had acknowledged and consented to the Bank's Data Privacy Policy, all of such pursuant to article 15(1)(a) to (h) of the GDPR*".

26. The Commissioner emphasises that compliance with the right of access should not be merely the provision of a copy of personal data undergoing processing, but also the provision of information in relation to the processing activity. The Court of Justice of the European Union (the "**CJEU**") held that article 15(1) and article 15(3) should not be treated as separate rights, but as one right. The CJEU stated that the "*first sentence of Article 15(3) of the GDPR cannot be interpreted as establishing a separate right from that provided for in Article 15(1) thereof*"[4].

27. To this end, the controller must provide a copy of the personal data undergoing processing, together with the information set forth in article 15(1)(a) to (h) and, where applicable, article 15(2) of the Regulation.

28. Whereas the majority of the information as set forth in article 15(1)(a) to (h) would generally be included in the data protection policy of the controller, however, the requirement in terms of article 15(1)(a) to (h) of the Regulation should not be treated as the same requirement imposed on the controller in terms of article 13 and article 14 of the Regulation. This is due to the fact that articles 13 and 14 of the Regulation are intended to provide *ex-ante* information to the data subjects, whereas article 15(1) of the Regulation is intended to provide *ex-post* information about the specific processing conducted by the controller in relation to the person exercising the right of access. Therefore, the information provided by the controller in terms of article 15(1)(a) to (h) of the Regulation must be tailored to address the specific processing conducted by the controller vis-à-vis the person requesting access. The EDPB Guidelines provide that:

> "*The third component of the right of access is the information on the processing and on data subjects' rights that the controller has to provide under Art. 15(1)(a) to (h) and 15(2). Such information could be based on text taken, for*

[4] Case C-487/21, F.F. vs Österreichische Datenschutzbehörde, decided on the 4th May 2023, paragraph 32.

example, from the privacy notice of the controller or from the controller's record of processing activities referred to in Art. 30 GDPR, ***but may have to be updated and tailored to the data subject's request***"[5] [emphasis has been added].

29. Furthermore, in a judgment delivered in January 2023, the CJEU emphasised the importance of article 15(1) of the Regulation, read in conjunction with recital 60 thereof, particularly, how the provision of information in relation to the processing operation is necessary for the data subject to understand how his personal data are being processed and to exercise other data protection rights in terms of Chapter III of the Regulation. The CJEU held that the information which the controller should provide to the data subject is a requirement which emanates from the principle of transparency:

> "*It follows from the above contextual analysis that Article 15(1)(c) of the GDPR is one of the provisions intended to ensure transparency vis-à-vis the data subject of the manner in which personal data are processed and enables that person, as the Advocate General observed in point 33 of his Opinion, to exercise the rights laid down, inter alia, in Articles 16 to 19, 21, 79 and 82 of the GDPR.*"[6]

30. This led the Commissioner to conclude that the controller failed to provide with its reply dated the 28th June 2024 the information in relation to the processing activity in terms of article 15(1)(a) to (h) of the Regulation, save for the information that the personal data of the complainant were not disclosed to third parties. Therefore, the Commissioner concludes that the manner how the controller handled the request of the complainant was not compliant with the principles of fairness and transparency as set forth in article 5(1)(a) of the Regulation and the reply of the 28th June 2024 infringed the second half of article 15(1) of the Regulation.

<u>The limitation imposed by the controller pursuant to article 15(4) of the Regulation</u>

31. In the reply dated the 5th July 2024, the controller informed the complainant that his right of access was partially limited on the basis that the "*internal communication is the sole property of* [redacted] *and cannot be shared with third parties, due to the fact that as per Article 15(4) of the GDPR this may adversely affect the rights and freedoms of others, particularly Bank officials, who are bound with professional and bank secrecy.*".

[5] ibid 2. paragraph 20.
[6] Case C-154/21, RW vs Österreichische Post AG, decided on 12th January 2023, paragraph 42.

32. As a preliminary consideration, the Commissioner noted that it is incorrect to argue that internal communications in the form of emails which contain personal data in relation to a data subject fall outside the scope of the right of access. The data subject should have the right to obtain a copy of his personal data irrespective as to where and how the data are stored by the controller. In a judgment delivered in October 2023, the CJEU held that:

> "*First of all, the Court has held that, according to its wording, the first sentence of Article 15(3) of the GDPR* ***confers on the data subject the right to obtain a faithful reproduction of his or her personal data, understood in a broad sense, that are subject to operations that can be classified as 'processing' carried out by the controller*** *(judgment of 4 May 2023, Österreichische Datenschutzbehörde and CRIF, C-487/21, EU:C:2023:369, paragraph 28).*" [7][emphasis has been added].

33. In the above-cited judgment, the CJEU clarified that the right of access should grant data subjects the right to obtain a faithful reproduction of their personal data. Therefore, for the right of access to apply, there must be 'personal data' in relation to a data subject within the meaning of article 4(1) of the Regulation and a 'processing operation' conducted by a controller in relation to that personal data within the meaning of article 4(2) thereof.

34. For the purpose of the Regulation, 'personal data' is defined as "*any information relating to an identified or identifiable natural person*" and 'processing' is an operation, or a set of operations applied to personal data, which could include, *inter alia*, collection, recording, storage or also consultation. The settled case-law of the CJEU applies a broad interpretation to these definitions. As a result, the scope of the Regulation has been broadened to safeguard the right to the protection of personal data. Therefore, in the present case, any internal emails exchanged between employees that contain the personal data of the complainant are deemed to be a processing operation which fall within the material scope of the Regulation.

35. As part of the investigation of this complaint, the Commissioner ordered the controller to provide a copy of the "*internal communication*" pursuant to his investigative power as set forth in article 58(1)(e) of the Regulation. On the 17th September 2024, the controller complied with the order of the Commissioner and provided a copy of the emails exchanged among its employees. Following a thorough examination of these emails, the Commissioner could note that not all emails contain personal data, however, there are some emails exchanged among

[7] Case C-307/22, FT vs DW, decided on the 26th October 2023, paragraph 71.

the employees that contain the personal data of the complainant within the meaning of article 4(1) of the Regulation. Therefore, for the purpose of this investigation, the Commissioner sought to establish whether the limitation invoked by the controller in terms of article 15(4) of the Regulation was indeed justified.

36. Article 15(4) of the Regulation states that the "*right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others*". This provision has to be read in light of recital 63 of the Regulation, which reads as follows: "[t]*hat right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject*".

37. Therefore, the right of access is subject to the limits that result from article 15(4) of the Regulation. The EDPB Guidelines shed further light on the applicability of this limitation:

> "*With regard to Recital 4 GDPR and the rationale behind Art. 52(1) of the European Charter of Fundamental Rights, the right to protection of personal data is not an absolute right. Hence also the exercise of the right of access has to be balanced against other fundamental rights in accordance with the principle of proportionality. When the Art. 15(4) GDPR assessment proves that complying with the request has adverse (negative) effects on other participants' rights and freedoms (step 1), the interests of all participants need to be weighed taking into account the specific circumstances of the case and in particular the likelihood and severity of the risks present in the communication of the data. The controller should try to reconcile the conflicting rights (step 2), for example through the implementation of appropriate measures mitigating the risk to the rights and freedoms of others. As emphasised in Recital 63, protecting the rights and freedoms of others by virtue of Art. 15(4) GDPR should not result in a refusal to provide all information to the data subject.* ***This means, for example, where the limitation applies, that information concerning others has to be rendered illegible as far as possible instead of refusing to provide a copy of the personal data***"[8] [emphasis has been added].

[8] ibid. 2, paragraph 173.

38. Accordingly, the Commissioner requested the controller to clearly explain which rights were or are to be adversely affected and who may be affected as a result of the disclosure of the requested personal data. Pursuant to the principle of accountability as set forth in article 5(2) of the Regulation, it remains the responsibility of the controller to effectively demonstrate that it has conducted a proper assessment, which led to the limitation of the right of access. In particular, the controller must be able to demonstrate that the rights or freedoms of others would be adversely affected in the specific situation. However, even if this is successful, as a general rule, the information should not be refused outright. In its submissions dated the 17th September 2024, the controller stated that the limitation was imposed to protect the personal data of its employees, who are bound by the professional and bank secrecy. The Commissioner recognises that the employees are bound by professional secrecy laws, however, the "*copies of internal correspondence shared via electronic mail between* [redacted] *employees regarding the formal OAFS complaint –* [redacted]" contain personal data pertaining to the complainant which were processed within the context of a complaint lodged by the complainant with the Office of the Arbiter for Financial Services case. Therefore, the professional secrecy laws should not hinder the complainant from accessing his own personal data which relates to a case that was *res judicata* at the time of receipt of the subject access request.

39. After assessing the contents of the email correspondence, the Commissioner determined that applying article 15(4) of the Regulation should not result in refusing to provide access to the emails exchanged among the employees that contain the personal data of the complainant altogether, but the controller should leave out or render illegible the names, email addresses, email signatures and any other personal data pertaining to its employees. This would reach a balance between the right of access pertaining to the complainant and the right to the protection of personal data pertaining to the employees of the controller.

On the basis of the foregoing considerations, the Commissioner is hereby deciding:

- **that the reply dated the 28th June 2024 failed to inform the complainant about the limitation invoked pursuant to article 15(4) of the Regulation in relation to the personal data contained in the "*internal correspondence shared via electronic mail between* [redacted] *Bank employees regarding the formal* [redacted]", and therefore, the reply of the controller lacked the necessary elements of transparency and fairness as required by the principles set forth in article 5(1)(a) of the Regulation;**

- **that the reply dated the 28th June 2024 failed to include information in relation to the processing activity as set forth in article 15(1)(a) to (h) of the Regulation, save for the information that the personal data of the complainant were not disclosed to third parties; and**

- **that the controller was not justified to limit the right of access pertaining to the complainant in terms of article 15(4) of the Regulation in relation to the personal data contained in the emails exchanged among the employees of the controller, and, therefore, the non-disclosure of this personal data led to an infringement of article 15(3) of the Regulation.**

By virtue of article 58(2)(b) of the Regulation, the Commissioner is issuing a reprimand to the controller for failing to comply with the provisions of the Regulation.

Pursuant to article 58(2)(c) of the Regulation, the Commissioner is ordering the controller to provide the complainant with information in relation to the processing activity pursuant to article 15(1)(a) to (h) of the Regulation, and access to the emails containing his personal data after redacting the personal data of the employees of the controller and other non-personal data.

For the purpose of providing the necessary assurances to the complainant, before providing him with the redacted version of the "*internal correspondence shared via electronic mail between* [redacted] *regarding the formal* [redacted], the controller shall consult the Commissioner on such version to ensure that it is consistent with this decision.

The controller shall comply with this order by no later than twenty (20) days from the date of service of this legally binding decision and inform the Commissioner of the action taken immediately thereafter.

Ian DEGUARA (Signature)
Digitally signed by Ian DEGUARA (Signature)
Date: 2025.01.14 15:14:48 +01'00'

Ian Deguara
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[9] 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*".

[9] Further information is made available on the website of this Office, which may be accessed on this hyperlink: https://idpc.org.mt/appeals-tribunal/