

COMPLAINT

1. On the 27th of June 2023 [REDACTED] the “**complainant**”), through his legal counsel, lodged a complaint against [REDACTED] (the “**controller**” or the “**Bank**”) with the Information and Data Protection Commissioner (the “**Commissioner**”) pursuant to article 77(1) of the General Data Protection Regulation¹ (the “**Regulation**”), alleging that the controller unlawfully accessed the complainant's bank account, and subsequently, disclosed his personal data with third-party entities.

ALLEGATIONS BY THE COMPLAINANT

2. For the purpose of this complaint, the Commissioner assessed the relevant allegations submitted by the complainant:
 - a. that during ongoing judicial proceedings between the parties, the complainant became aware that the controller had utilised its position with the aim of benefiting itself as an employer;
 - b. that the Bank's access to and visibility of the complainant's transactions contributed to the complainant's suspicion;

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.

- c. that the visibility and processing of data, which are the subject of the complaint, would not have been feasible had the Bank not been the complainant's employer or had the complainant utilised another bank account with a different financial institution; and
 - d. that the evidence supporting the complaint is to be procured from the Bank, as the Industrial Tribunal had issued an order for the documents to remain sealed and accessible exclusively to the involved parties in the case.
3. For the purpose of analysing this case, the Commissioner divided the complaint into two (2) distinct parts:
 - a. the lawful basis to access the complainant's bank account; and
 - b. the disclosure of the complainant's personal data to third parties.

INVESTIGATION

4. Upon evaluating the complaint, the Commissioner requested the complainant to specify the alleged third party and provide supporting evidence for such assertion. The complainant stated that the Bank had disclosed the complainant's personal data to the [REDACTED] and contended that this group comprises individuals not employed by the Bank. Furthermore, the complainant maintained that such data processing is substantiated by the document referenced in the complaint.

Request for submissions

5. On the 6th of July 2023, in accordance with article 58(1)(a) of the Regulation and the internal investigative procedure of this Office, the Commissioner requested the controller to provide its submissions regarding the complaint, along with any other pertinent information it deemed relevant and necessary in relation to the allegations made by the complainant.
6. On the 4th of August 2023, the controller presented the following principal arguments for the Commissioner's consideration in the legal analysis of the case. Given that the complainant has already been furnished with these submissions, only the arguments pertinent to the legal analysis of the case will be outlined in this section.

Lawfulness of the Processing

7. The Bank asserted that it had reasonable suspicions of financial misconduct or wrongdoing on the part of the complainant. Consequently, the Bank contended that it was justified in investigating the complainant, a procedure akin to its scrutiny of any individual holding an account with the Bank. The Bank further stated that it possessed legitimate apprehensions regarding potential financial crimes associated with the complainant's behaviour. These concerns were substantiated by various violations identified and validated in the report compiled by the [REDACTED] investigative unit within [REDACTED] based in [REDACTED] [REDACTED], (the [REDACTED] which posed a significant risk to the [REDACTED]
8. The controller emphasised that it has the obligation to report its investigative findings to the [REDACTED] (the "[REDACTED]") upon encountering potential misconduct by its employees. Moreover, it held that correspondence exchanged in writing between the Bank and the [REDACTED] provided evidence of [REDACTED] concerns regarding the matter.

Disclosure to third parties

9. In addition, the Bank asserted that, in the current complaint, the complainant's bank accounts were not accessed by the Bank's human resources department or any department responsible for evaluating compliance with employment contracts or employment conditions pertaining to the Bank's employees. The Bank clarified that access to his bank accounts was exclusively granted to the Bank's investigative units, namely to the [REDACTED] [REDACTED] and to the Bank's internal legal investigators, [REDACTED]. Furthermore, the controller confirmed that no third parties outside of the Bank were ever granted such access.
10. The Bank explained that the [REDACTED] report "*was originally drafted, under legal privilege, as an internal document by the [REDACTED]*", thus "*drafted by an internal investigative team of qualified individuals including legal counsel all employed by the [REDACTED] itself*". In this context, the Bank refuted the complainant's assertion that it processed the complainant's personal data to third parties in any manner: "*no entities of any kind outside of [REDACTED] except courts/tribunals, public authorities such as the [REDACTED] and the IDPC itself) were ever given and/or will be given access, by [REDACTED] to this document*".

11. The Bank concluded by expressing its willingness to provide the [REDACTED] Report to the Commissioner, along with the correspondence exchanged with the [REDACTED].

Submissions of the complainant

12. On the 5th of September 2023, the Commissioner provided the complainant with the opportunity to rebut the arguments made by the controller. By means of a communication dated the 20th of September 2023, the complainant submitted the following principal arguments:

Lawfulness of the Processing

13. The complainant contended that the Bank's inquiry into the plaintiff's bank accounts did not stem from suspicions of money laundering or financial crimes; rather, it was solely prompted by concerns "*due to a suspicion of a Conflict of Interest*".
14. In the event of genuine suspicions of money laundering, failure to submit a suspicious activity report or a suspicious transaction report to the [REDACTED] while solely notifying the [REDACTED] constitutes an incomplete action, and therefore, failing to report such suspicions would amount to a criminal offence.
15. Additionally, the complainant asserted that the processing of such information must adhere to consistent and transparent protocols, which was evidently not the case in this instance. The complainant had never been notified by the Bank regarding the scrutiny of his account for such reasons. Furthermore, the complainant argued that if he held accounts with a different institution, the employer, acting as the controller, would not have had access to transactional data unless explicit consent was obtained, or specific legal procedures were followed. Leveraging data from its banking division for employment-related investigations represents a clear violation of data protection laws, both ethically and legally.

Disclosure to third parties

16. The complainant maintained that although the entities involved in processing the subject matter of this complaint may be affiliated within the same corporate structure, each subsidiary or entity constitutes a distinct legal entity. Consequently, sharing information across these boundaries raises significant concerns regarding data protection.

17. Moreover, the complainant held that to transfer personal data between distinct legal entities, explicit consent, a legal obligation, or another clearly defined lawful basis is required. The mere relationship between companies under the same corporate umbrella does not inherently establish such a basis.

Further submissions provided by the controller

18. In line with the Commissioner's internal complaint-handling procedure, the controller was provided with the final opportunity to rebut the arguments made by the complainant. On the 13th of October 2023, the controller submitted the following salient arguments to address the submissions of the complainant:

- a. that the Bank firmly reaffirms its submissions and categorically refutes all of the complainant's allegations;
- b. that processing operations conducted for investigations by its legal counsel do not necessitate consent and requiring consent would render investigations impractical as targets would likely withhold such consent. Additionally, legal obligations often prohibit controllers from alerting targets about ongoing investigations; and
- c. that contrary to the complainant's assertion, the Bank possesses evidence in the form of a letter dated the 28th of February 2017, from the [REDACTED] to the Bank. This letter indicates that the [REDACTED] had been involved in numerous matters concerning the complainant from the outset and had requested follow-ups on these matters. The Bank asserts that this letter unequivocally justifies its conduct in carrying out the internal investigation in question.

19. The Bank concluded by extending an invitation to the Commissioner to review both the [REDACTED] report and the aforementioned [REDACTED] letter. The Bank stated that a decision made without thoroughly examining these pivotal documents would overlook crucial factors essential to the present case.

Meeting convened by the Commissioner

20. After reviewing the submissions presented by the involved parties, the Commissioner requested a meeting with the controller to examine the [REDACTED] report dated the 16th June 2016 and the correspondence exchanged between the [REDACTED] and the Bank, in particular the letter sent by the [REDACTED] dated the 28th of February 2017.

21. On the 6th of December 2023, a meeting was held with the Bank, during which the Commissioner was granted physical access to the [REDACTED] report. The Commissioner observed that, in their investigation, the [REDACTED] specifically focused on two aspects – first, to identify potential breaches of policies and procedures by the complainant in relation to activities leading to lack of due diligence, sharing confidential information and negligence to adhere to internal sanction policies, and secondly to assess potential conflicts of interest arising from the role of the complainant.
22. The [REDACTED] Report concluded that based on its findings, along with those from preliminary investigations conducted by the [REDACTED] and the [REDACTED] departments, the complainant should be suspended.
23. Furthermore, during the meeting held with the Commissioner, the Bank was requested to substantiate its assertion, as stated in its submissions dated the 4th of August 2023, regarding the concerns expressed by the [REDACTED] in connection with the complainant. The Bank asserted that, when it submitted the [REDACTED] Report to the [REDACTED] on the 18th of July 2016, it demonstrated its interest. Additionally, the controller noted that in the letter dated the 28th of February 2017, which was also accessed and inspected by the Commissioner, the [REDACTED] had requested various clarifications and additional documents.

LEGAL ANALYSIS AND DECISION

24. The Commissioner observed that the purported infringements occurred before the coming into force of the Regulation. Article 34 of Cap. 586 states that the previous data protection legislation, namely Cap. 440 of the Laws of Malta, shall be repealed save for those instances covered by article 34(2)(a) of Cap. 586 of the Laws of Malta. This provision states that Cap. 440 “*shall remain in force for the purpose of any act, decision, action or proceedings taken in respect of any breach of the repealed Act that occurred or were instituted prior to the coming into force of this Act*”. Therefore, in the present case, the applicable legislation is the Data Protection Act, Cap. 440 of the Laws of Malta (the “Act”).

Lawfulness of the Processing

25. For the purpose of this complaint, the Commissioner proceeded to determine whether the controller had a valid lawful basis pursuant to article 9 of the Act to access the complainant’s bank accounts and to disclose such data to third parties.

26. The Court of Justice of the European Union (the “CJEU”) held that “*Article 7 of Directive 95/46 sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as being lawful and that the Member States cannot add new principles relating to the lawfulness of the processing of personal data or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in that article*”².
27. The Commissioner proceeded to examine the Prevention of Money Laundering Act, (Cap. 373 of the Laws of Malta) (the “PMLA”) which designates the [REDACTED] as an agent of the [REDACTED] (the [REDACTED]), obliging the [REDACTED] to offer assistance and cooperation to the [REDACTED] in executing its duties under the [REDACTED]. Consequently, the Commissioner observed that in its capacity as an agent of the [REDACTED] the [REDACTED] collaborates with and acts on behalf of the [REDACTED] in the enforcement of the [REDACTED] Terrorism measures.
28. The Commissioner emphasises that despite the fact that the complainant is an employee of the Bank, the complainant also holds the status of a customer by virtue of maintaining bank accounts. Pertinently, upon establishment of a business relationship, regulation 7(1)(d) of the Subsidiary Legislation 373.01 Prevention of Money Laundering and Funding of Terrorism Regulations (the “PMLFTR”) mandates subject entities, such as the Bank, to conduct continuous monitoring. Such monitoring encompasses two primary aspects: (a) scrutiny of transactions; and (b) the maintenance of current information, documentation, and data related to the customer. Regarding transaction scrutiny, reference is made to the Financial Intelligence Analysis Unit Implementing Procedures³, which delineate that “*the scrutiny of transactions through transaction monitoring consists in using the subject person's knowledge of the customer (including the information gathered on the purpose and intended nature of the business relationship and the customer's business and risk profile) to identify any transactions that are unusual*”⁴.
29. Furthermore, the PMLFTR explicitly requires subject persons to examine the purpose and background of all complex and unusually large transactions and unusual patterns of transactions that do not have any apparent or economic lawful purpose and increase the degree and nature of ongoing monitoring to determine whether the transactions are suspicious⁵.

² Case C-582/14, Patrick Breyer vs Bundesrepublik Deutschland, decided on the 19th October 2016, para. 57.

³ Issued by the Finance Intelligence Analysis Unit in terms of the provisions of the Prevention of Money Laundering Regulations (S.L. 373.01) PART I, first issued on 20 May 2011, last amended on 18th October 2021.

⁴ Ibid 2, page 137

⁵ Regulation 11(9) PMLFTR.

30. In light of the foregoing, the Commissioner proceeded to evaluate the Bank's submissions, contending that it had reasonable suspicions of financial misconduct or wrongdoing on the part of the complainant. Additionally, the Bank elucidated its obligation to relay the investigative findings to the [REDACTED] upon encountering potential misconduct by its employees. Furthermore, the Bank asserted that the said suspicions were subsequently validated in the [REDACTED] Report.
31. Conversely, the complainant contended that the Bank's investigation into his bank account was not driven by suspicions of money laundering or financial wrongdoing but rather stemmed from a conflict-of-interest apprehension. In this context, the Commissioner scrutinised the [REDACTED] Report and ascertained that the document identified several deficiencies pertaining to the complainant⁶, thereby confirming the Bank's reasonable suspicion of financial crime perpetrated by the complainant and this therefore justified access to his accounts.
32. In this regard, the Commissioner considers that the Bank had a legal obligation to examine unusual and suspicious transactions, and therefore, the processing activity is deemed to be lawful in terms of article 9(c) of Cap. 440 of the Laws of Malta.

Disclosure to third parties

33. Furthermore, the complainant alleged that the Bank had disclosed his transaction data to third parties, specifically [REDACTED]. The Commissioner acknowledged the Bank's assertion that access to the mentioned accounts was exclusively granted to the bank's investigative units, namely the [REDACTED] and the [REDACTED] at [REDACTED].
34. The Commissioner sought to determine whether [REDACTED] had indeed accessed the complainant's accounts. To this end, the Commissioner received a confirmation from the Bank, via an email dated the 20th of February 2024, stating that [REDACTED] *have not been given access to [REDACTED] Malta systems. However, as part of the investigation I (the [REDACTED] gave them supporting evidence including statements where I did find concerns*". Following receipt of this statement, the Commissioner requested clarification regarding the term "statements," particularly whether it referred to 'bank statements' or 'written statements' issued by the [REDACTED]. [REDACTED] Furthermore, the Commissioner stipulated that such confirmation and clarification should be provided under oath.

⁶ Paragraph 21, page 7 of this decision.

35. On the 26th of March 2024, the Bank submitted its affidavit, whereby the Head of [REDACTED] stated that [REDACTED] have not been given access to [REDACTED] Systems. However, as part of the investigation I gave them supporting evidence including statements where I did find concerns and I confirm that 'statements' included bank statements. These were used as supporting evidence to transactions that had Financial Crime red flags". Following this confirmation, the Commissioner sought in essence to examine whether the controller unlawfully disclosed the complainant's statements to [REDACTED]
36. The controller submitted that if a transaction carried out by any of the Bank's employees leads to the identification of potential financial crime(s), this information may also be shared by the [REDACTED] to Human Resources (the "HR") to initiate an investigation in accordance with standard HR protocols. This may include procedures for addressing potential misconduct, as outlined in the Collective Agreement, and taking any necessary disciplinary action against the employee. Moreover, it held that employees are informed of such procedures by means of the employees' privacy notices, the collective agreement and HR Manual and procedures, which are all available through the Bank's HR Portal.
37. Given this context, on the 15th of April 2024, the Commissioner requested the Bank to provide the aforementioned documents. Furthermore, the Commissioner requested the Bank to submit additional documents and, or information to clarify the nature of its relationship with [REDACTED] as well as the type of information shared with employees regarding this relationship.
38. On the 18th April 2024, the Bank submitted extracts from its HR Manual and also from the Collective Agreement signed with [REDACTED] concerning disciplinary procedures. The Commissioner noted that these documents stipulate that the Bank must adhere to its rules and regulations, uphold proper standards of performance and behaviour, and maintain the highest levels of integrity both within and outside the Bank. Furthermore, these documents state that the Bank has the authority to enforce discipline among all its employees and to conduct thorough investigations to establish the facts as part of maintaining proper discipline.
39. Additionally, the Bank provided the 'HR Worker Data Privacy Notice' and highlighted that on page 7, under the section titled 'Who we might share your information with,' employees are informed that their information may be shared with "other [REDACTED] companies and any sub-contractors, agents, or service providers who work for us or provide services to us or other

██████████ companies (including their employees, sub-contractors, service providers, directors, and officers).”

40. In response to the Commissioner’s request, the Bank submitted its ██████████ ██████████ Agreement,’ which is entered into between ██████████ and other members of the ██████████. This agreement specifies that the “Data Provider agrees to transfer to the Data Recipient and/or allow the Data Recipient to access the Data, and the Data Recipient agrees to receive, access, and otherwise Process the Data in accordance with the terms of this Agreement.”.

41. Despite the submission of these documents, the Commissioner could not find any reference to the ██████████. Consequently, the Commissioner requested the Bank to direct him to the specific section explaining its relationship with ██████████. In an email dated the 3rd May 2024, the Bank explained that the local ██████████ department initiates investigations related to the prevention of financial crimes. However, when the nature and complexity of the investigations require a higher level of legal expertise, the head of the business or the executive management may decide to engage the ██████████. The Bank explained that ██████████ is a pool of ██████████ within the ██████████. The Bank concluded that the HR Manual does not specify the types of investigations, but it generally informs, along with the Privacy Notice, that any infringement may be subject to internal investigations and that employees’ data may be shared for this purpose with the ██████████ and with other parties involved in the investigations.

42. Upon receiving this information, the Commissioner requested clarification from the Bank regarding the functional role of the ██████████. Specifically, the inquiry focused on whether the ██████████ is classified as an independent controller or as a processor of the Bank. The Bank confirmed that the legal relationship between the Bank and ██████████ was one of a controller-processor, as delineated in the ██████████ (the “Agreement”). The Bank referred to the Agreement, which had previously been submitted to the Commissioner, noting that the Bank is explicitly listed as one of the ‘Companies’ in Schedule A. Furthermore, among the services provided by ██████████ to these Companies, Schedule D specifies the “provision of a variety of legal services” as well as “provision of a variety of internal audit services”.

43. Moreover, the Bank asserted that the Agreement, specifically the controller-processor agreement, met the legal requirements which were set out in the Act. It cited Clauses 2.5 and 5.2, which clearly stipulate that ██████████ shall act solely under the instructions of the Bank.

Additionally, the Agreement imposes an obligation on ██████████ to implement stringent security measures to ensure the integrity and confidentiality of the data while in its possession, thereby preventing unauthorised or accidental recording, disclosure, processing, deletion, alteration, use, or any form of tampering with the data.

44. The Bank further maintained that the Agreement encompasses obligations that exceed the statutory requirements. These obligations include, among others, explicit descriptions of data ownership (which unequivocally remains with the controller and not the processor)⁷, a requirement to return the data to the controller upon request or upon termination of the Agreement, and strict controls over sub-processing, which must be conducted in accordance with the Agreement and under a subcontracting/sub-processing agreement⁸.
45. In conclusion, the Bank determined that it was not necessary to obtain the consent of the complainant in order to engage a third party acting as a data processor for the purpose of conducting the aforementioned investigation.
46. Upon reviewing the documents submitted by the Bank, particularly the Agreement and its accompanying explanation, the Commissioner concludes that the processing of the complainant's personal data by ██████████ is lawful and in compliance with articles 25 and 26 of the Act. This processing was conducted in accordance with the Bank's established procedures and aligns with article 9(f) of the Act, as by virtue of the Agreement, the processing was necessary to serve the legitimate interest pursued by the Bank.

Information to Data Subject

47. Article 19 of the Act requires that the data subjects are informed by the controller about the details of the processing at the time when the controller collects the data directly from the data subject. This enshrines a positive obligation on the controller, which requires that the controller provides a set of required details about the processing operation, which is usually contained in a data protection policy, which includes, *inter alia*, the identity and contact details of the controller, the purposes of the processing for which the personal data are intended, the legal basis for the processing, the storage period, and the right to exercise the data subjects' rights.

⁷ Clause 5.1

⁸ Clause 13.2

48. Furthermore, Article 29 Working Party provides that the information contained in article 13 and 14 of the Regulation should generally be contained in a written notice, and in fact, it provides that *“the notice containing such information is frequently referred to as a data protection notice, privacy notice, privacy policy, privacy statement or fair processing notice. The GDPR does not prescribe the format or modality by which such information should be provided to the data subject but does make it clear that it is the data controller’s responsibility to take “appropriate measures” in relation to the provision of the required information for transparency purposes.”*⁹
49. During the investigation, the controller submitted the HR Manual and the Collective Agreement with [REDACTED] which regulate disciplinary procedures, and which are available on its intranet. Additionally, the HR Worker Data Privacy Notice informs employees that any infringement may be subject to internal investigations and that employees’ data may be shared for this purpose with the [REDACTED] and other parties involved in the investigations. The Commissioner therefore concludes that, for the purpose of the transparency principle, the complainant is informed that the Bank may share his data with the [REDACTED] during course of internal investigations.

On the basis of the foregoing considerations, the Commissioner hereby decides that the controller has processed the personal data of the complainant in accordance with a lawful basis under article 9 of the Data Protection Act (Cap.440 of the Laws of Malta) and has also provided him with the necessary information pursuant to article 19 thereof.

The Commissioner dismisses the complainant’s allegations in their entirety.

Ian
DEGUARA
(Signature)

Digitally signed
by Ian DEGUARA
(Signature)
Date: 2024.11.14
09:51:01 +01'00'

Ian Deguara
Information and Data Protection Commissioner

⁹ Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679, as last revised and adopted on the 11th April 2018.

Right of Appeal

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 in writing to the Tribunal within twenty days from the service of the said decision as provided in article 23”*.

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

