

[REDACTED]

vs

[REDACTED]

**COMPLAINT**

1. On the 14<sup>th</sup> of May 2025, [REDACTED] (the “complainant”) lodged a data protection complaint with the Information and Data Protection Commissioner (the “Commissioner”) pursuant to article 77(1) of the General Data Protection Regulation<sup>1</sup> (the “Regulation”), alleging that, in order to send bill payments to [REDACTED] [REDACTED] (the “controller” or [REDACTED] through the ‘Pay a Bill’ portal on the [REDACTED] [REDACTED] online banking application, [REDACTED] required him to provide his mobile number in a mandatory data field on the portal. The complainant further alleged that the portal does not allow him to proceed with sending the payment unless the mobile number is provided. In light of this, the complainant requested the Commissioner to order the controller either to remove the data field entirely, or to make the provision of this personal data optional rather than mandatory, arguing that it is not necessary for this personal data to be collected by the controller in order to process bill payments.
2. For the purpose of supporting his allegation, the complainant submitted a copy of the screenshot of the controller’s payment form on [REDACTED] online banking application, which demonstrates that in order to send a payment for a payment owed to the controller, the following information must be provided:

---

<sup>1</sup> 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.

[REDACTED]

- i. "Account Number";
- ii. "Invoice Number";
- iii. "Mobile Number"; and
- iv. "Amount".

## INVESTIGATION

### Preliminary considerations

3. Preliminarily, in the process of assessing the admissibility of the complaint, the Commissioner sought to determine whether the controller of the personal data is ██████ being the organisation which receives the bill payments, or whether it is ██████ being the organisation which hosts the application through which the complainant sent the bill payments to ██████. The Commissioner therefore had to establish which entity determined the means and purposes of the processing of the data. To this end, the Commissioner requested ██████ to provide clarification regarding its role, if any, in determining what personal data is collected from users when sending bill payments to organisations via the 'Pay a Bill' portal, or whether this determination is made independently by each of the organisations listed on the portal.
4. By means of an email sent on the 9<sup>th</sup> of June 2025, ██████ submitted the following statement in response to the Commissioner's request:

*"The Bank does not decide what information the service provider (in this case, ██████) needs. It is the service provider who instructs the Bank what information to collect. Other than that, nothing. The Bank acts on the instructions of the service provider."*

5. After receiving ██████ statement, the Commissioner proceeded to examine the 'Pay a Bill' portal directly. Upon examining the portal, the Commissioner found that the data fields which had to be filled in by users in the various organisations' payment forms were not the same, but varied, such that each organisation was requesting different information depending on the nature of service it provided. Accordingly, the Commissioner concluded that ██████ determines the means and purposes of the processing of the personal data, and does indeed assume the functional role of a controller within the meaning of article 4(7) of the Regulation.

Request for submissions

6. By means of an email sent on the 11<sup>th</sup> of June 2025, the controller was provided with a copy of the complaint, and was requested to put forward its submissions that it deemed relevant and necessary to defend itself against the allegation made by the complainant. Pursuant to article 58(1)(e) of the Regulation, the Commissioner ordered the controller to provide a justified explanation as to why the controller considers it necessary to require users to provide their mobile number in order to send bill payments to the controller. The controller was informed that its submissions should be made within twenty (20) days.
7. On the 1<sup>st</sup> of July 2025, upon the lapse of the twenty (20) day period, the controller had not provided any form of response to the Commissioner's communication. Although an email was sent on the same day reminding the controller to respond, no response was received by the controller. Thereafter, several email reminders were sent to the controller on multiple email addresses between July and August 2025. Although automated acknowledgement emails were received immediately after sending these reminders, confirming that the emails had been successfully delivered to the controller, no response was provided by a member of staff of the controller.
8. On the 7<sup>th</sup> of August 2025, using a contact number listed on the controller's website, this Office attempted to reach out to the controller by phone. The phone call was answered by a member of the controller's customer care staff, who instructed this Office to forward the emails to another email address of the controller, and assured this Office that a response would be provided in a prompt manner. Accordingly, on the same day, the thread of emails containing (i) the request for the controller's submissions, and (ii) the various reminders sent thereafter, were forwarded to the email address provided. This Office did not receive any response to this email. Additionally, on the same day, an email was also sent to the controller's chief executive officer, to draw his attention to the complaint lodged against it and to the Commissioner's request for submissions.

Submissions of the controller

9. By means of an email sent on the 30<sup>th</sup> of August 2025, the controller responded, and made the following submissions for the Commissioner to consider in the legal analysis of the present case:

- a. that *"after having investigated the matter, I wish to draw attention that, contrary to what [REDACTED] have indicated, this field was specifically request by [REDACTED] to be able to clarify with the clients any problematic payments"*;
- b. that *"additionally, the inclusion of a contact number field facilitates matters for [REDACTED] whenever there are any issues with payments since the customer can be contacted directly. Such data is for the benefit of all customers including the complainant himself"*; and
- c. that *"there are instances where clients themselves forget to include payment references when making payments via internet banking. Likewise, in such cases the client can be contacted so that the payment will be allocated correctly."*

10. In view of the fact that the controller refuted that it was responsible for what was alleged in the complaint, the controller was given the opportunity to put forward any additional submissions or evidence to justify its position and to defend itself against the allegation made by the complainant. By means of an email sent on the 30<sup>th</sup> of September 2025, the controller informed the Commissioner of its intention to put forward additional submissions. Although the controller was clearly informed to put forward its submissions at the earliest, on the 13<sup>th</sup> of October 2025, a further reminder had to be sent to the controller.

11. By means of an email sent on the 17<sup>th</sup> of October 2025, the controller submitted the following arguments for the Commissioner to consider during the legal analysis of the case:

- a. that *"primarily, as the complainant himself has stated, the platform which is requiring personal data of the complainant pertains to [REDACTED] and not [REDACTED]"*;
- b. that *"as previously intimated, this field was specifically requested by [REDACTED] back when it offered payment services to [REDACTED] the reason being that whenever a payment is made, a contact number is indicated such that in the event of any erroneous transactions, the person making the transaction is easily contacted"*;
- c. that *"the inclusion of a mobile number is not only beneficial to [REDACTED] to enable it to contact an individual in case of such erroneous transactions, but also beneficial to the individual himself/herself in that he or she can easily be informed of any suspicious activity/payments which may be made."* ;

- d. that the “use of [REDACTED] platform is optional not mandatory as there are other means through which an individual may pay an invoice, including directly through [REDACTED] [REDACTED] online platform”; and
- e. that, therefore, “in the circumstances, [the controller] deems that the inclusion of the contact number is not excessive but justified.”

Submissions of the complainant

12. The Commissioner shared the submissions of the controller with the complainant to provide him with the opportunity to respond to, and rebut the arguments presented. In response, the complainant made the following submissions which were pertinent to the complaint:

- a. that, in response to the controller’s submissions that it was not responsible for determining what personal data is requested from users when sending bill payments, as this determination is made by [REDACTED] the complainant argued that this was untruthful, and submitted, “why would [REDACTED] require my mobile number to pay [the controller], but not likewise require this exact, same information when I wish to pay some other company?” ;
- b. that, in response to the controller’s submissions that requiring users to provide their mobile number in order to send bill payments “facilitates matters for [the controller]”, the complainant submitted that the controller’s statement clearly implies that it is indeed the controller that expects this personal data to be provided, not [REDACTED]
- c. that, in response to the controller’s submissions that “there are instances where clients themselves forget to include payment references when making payments via internet banking” and that “in such cases the client can be contacted so that the payment will be allocated correctly”, the complainant submitted that the controller is already in possession of information which could be used to contact the client in these instances, such as the client’s email address or postal address;
- d. that, in response to the controller’s submissions that “the platform which is requiring the personal data of the complainant pertains to [REDACTED] and not [the controller]”, the complainant submitted that since “other entities do not ask

*for one's mobile when bills are to be paid, it is abundantly clear that [REDACTED] are themselves requiring (not as an option, mind) this additional information to be submitted"; and*

- e. that, in response to the controller's submissions that the "use of [REDACTED] platform is optional not mandatory as there are other means through which an individual may pay an invoice, including directly through [the controller's] online platform", the complainant submitted that it should be in the controller's interest to make all modern means available to its clients for the purpose of easily and safely paying their bills to the controller, and that clients should still be able to use the [REDACTED] application for this purpose, but without having to provide their mobile number, reiterating that this is "excessive and unjustified".

13. Finally, the Commissioner shared the complainant's rebuttal with the controller to provide it with the opportunity to address the arguments presented. The controller did not submit any response.

## LEGAL ANALYSIS AND DECISION

### The Controller's Lack of Cooperation

14. Before proceeding to analyse the merits of the present case, the Commissioner considered it necessary to address the persistent lack of cooperation exhibited by the controller during the course of the investigation of the complaint, evidenced in particular by the controller's excessive delay in responding to the Commissioner's communications. In this regard, the Commissioner highlighted that article 31 of the Regulation places a clear obligation on the controller to cooperate with the Commissioner in the performance of his tasks. This includes the investigative tasks of the Commissioner pursuant to article 57(1)(f) of the Regulation, namely, to investigate the complaint lodged by the data subject and to inform the data subject of the progress and outcome of the investigation within a reasonable period. The controller's failure to respond to the multiple communications which were sent in a timely and comprehensive manner unnecessarily delayed the investigation.
15. Furthermore, the Commissioner considered the controller's lack of cooperation to be of heightened concern and expected the controller to be fully aware of its obligations and

responsibilities under the Regulation. Accordingly, in addition to the unnecessary delays caused in concluding the investigation, the Commissioner noted that the controller's lack of cooperation also raises serious doubts regarding its governance structure which is indeed essential to ensure that engagement with a national regulatory authority, in particular during the course of a formal or official investigation, is taken seriously and in timely and professional manner.

### The Principle of Data Minimisation

16. Article 5(1)(c) of the Regulation establishes the principle of data minimisation, and states that the personal data processed by the controller shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*". This principle is further reinforced by recital 39 of the Regulation, which states that "*personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.*" In addition, article 25(2) of the Regulation places an obligation on the controller to ensure that, by default, only the personal data which is strictly necessary for the specific purpose of the processing operation is processed. Collectively, these provisions stress the controller's responsibility to minimise the interference with the individual's fundamental right to the protection of personal data, by aiming to reduce the personal data collected to the lowest degree possible whilst still effectively achieving the purpose of the processing.

17. Accordingly, the scope of the Commissioner's legal analysis in the present case is to determine whether the controller's processing of the complainant's mobile number complied with the principle of data minimisation under the Regulation, or whether it went beyond what was genuinely necessary for the purpose of the processing. As part of this legal analysis, the Commissioner sought to examine the guidance provided by the European Data Protection Board (the "EDPB") on how controllers are expected to apply the principle of data minimisation in practice. In particular, the Commissioner referred to the EDPB's Guidelines 4/2019 on Data Protection by Design and by Default, which explain that "*controllers should first of all determine whether they even need to process personal data for their relevant purposes*", and that, "*the controller should verify **whether the relevant purposes can be achieved by processing less personal data***" [emphasis has been added].<sup>4</sup>

---

<sup>4</sup> European Data Protection Board Guidelines 4/2019 on Data Protection by Design and by Default, adopted on the 20<sup>th</sup> October 2020, paragraph 74.

18. The Commissioner also noted that in the Guidelines, the EDPB recognises the intrinsic link between the principle of data minimisation and the concept of ‘necessity’ in the Regulation. In this regard, the Guidelines explicitly state that:

*“Each personal data category shall be **necessary** for the specified purposes and should only be processed if it is not possible to fulfil the purpose by other means.”<sup>5</sup> [emphasis has been added].*

Accordingly, before collecting any personal data from the data subject, the controller must clearly identify the specific objective being pursued and must then assess whether the processing of that personal data is actually a necessary and effective way of achieving that objective. The Commissioner explained that in making this assessment, the controller must judiciously assess whether the personal data is strictly necessary to achieve its intended objective, as well as whether there are any less intrusive means available that could effectively achieve the same objective.

19. The requirement of necessity has also been recognised by the Court of Justice of the European Union (the “CJEU”). In its judgments, the CJEU has consistently held that where the processing of personal data is based on a legal ground other than the consent of the data subject under article 6(1)(a) of the Regulation, the processing must be shown to be necessary for the purpose being pursued, as set out in the wording of the other legal grounds for processing under article 6(1)(b) to (f) of the Regulation. In fact, in a recent judgement, the CJEU held that:

*“First, as is apparent from such Article 6, where the data subject has not given consent to the processing of his or her personal data for one or more specific purposes, in accordance with Article 6(1)(a) of Regulation 2016/679, the processing must, as is apparent from Article 6(1)(b) to (f), satisfy a requirement of necessity.*

*Second, such a requirement of necessity follows also from the principle of ‘data minimisation’, laid down in Article 5(1)(c) of that regulation, under which personal data are to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.”*  
[emphasis has been added].<sup>6</sup>

---

<sup>5</sup> Ibid. paragraph 76.

<sup>6</sup> Case C-77/21, Digi Távközlési és Szolgáltató Kft. vs Nemzeti Adatvédelmi és Információszabadság Hatóság, judgment of the Court (First Chamber) of the 20th October 2022, paragraphs 57 - 58.

20. In addition to the ‘necessity’ of the processing, the CJEU has held that the concept of ‘proportionality’ also gives expression to principle of data minimisation.<sup>7</sup> In this regard, the Commissioner noted that the principle of proportionality is a well-established legal concept under EU law which, in essence, requires that the advantages of a measure should not be outweighed by its disadvantages.<sup>8</sup> Accordingly, in the context of data protection, the extent of personal data processed must be fairly balanced against the intended purpose of the processing, to ensure that the processing does not disproportionately interfere with the rights of the data subject, which must be duly safeguarded.
21. Finally, the Commissioner also referred to the principle of accountability set out in article 5(2) of the Regulation, which provides that the controller is responsible not only for complying with the principles of data protection, but also for demonstrating that compliance in practice. In this regard, the EDPB’s Guidelines 4/2019 describe ‘accountability’ as an overarching principle,<sup>9</sup> which entails that the controller clearly understands its data protection obligations under the Regulation, and is able to comply with these obligations and implement them in practice.<sup>10</sup> In particular, with regard to the collection of personal data through computer programs or software applications, as in the present case, the EDPB in its Guidelines 4/2019 also highlights that “*by default, the controller shall not collect more data than is necessary*”, and that settings and options through which personal data are collected should be configured in such a way that “*only processing that is strictly necessary to achieve the set, lawful purpose is carried out by default*”.<sup>11</sup>
22. In the present case, the processing operation consisted in the collection of the mobile number of the complainant whenever a bill payment is sent to the controller through the ‘*Pay a Bill*’ portal on [REDACTED] online banking application. During the course of the investigation, when the Commissioner requested the controller to justify why it deemed it necessary to collect the data subject’s mobile number for the purpose of settling a bill payment, the controller submitted that having the mobile number is beneficial, as it may be used for the purpose of informing the data subject in the event that the data subject makes a payment in error, or in the event that other

---

<sup>7</sup> Case C-268/21, *Norra Stockholm Bygg AB v Per Nycander AB*, judgment of the Court (Third Chamber) of the 2nd March 2023, paragraph 54.

<sup>8</sup> European Data Protection Supervisor Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, page 9.

<sup>9</sup> European Data Protection Board Guidelines 4/2019, paragraph 64.

<sup>10</sup> *Ibid.* paragraph 88.

<sup>11</sup> *Ibid.* paragraph 42.

suspicious payment activity is detected, and maintained that therefore, the collection of the mobile number “*is not excessive, but justified*”.

23. The Commissioner considered that the controller’s stated purpose, namely, to inform the data subject in the event that an erroneous or suspicious payment is detected, would likely only arise in limited circumstances. Yet, the controller requires the mobile number to be provided in a compulsory manner for every transaction made through the portal. Consequently, the portal does not allow the transaction to be completed unless this personal data is provided. The Commissioner noted that the data subjects have to provide other data in addition to their mobile number, specifically, the ‘account number’, the ‘invoice number’, and the ‘amount’ of the payment. The Commissioner considers that the account number should, in itself, have been sufficient to identify the account associated with a given payment. In the event of any issue concerning a payment, the controller could match the account number with the contact details of the registered account holder already maintained in the systems.
24. Moreover, in its submissions, the controller stated that the “*use of the [REDACTED] platform is optional not mandatory as there are other means through which an individual may pay an invoice, including directly through [REDACTED] online platform*” [emphasis has been added]. In this regard, the Commissioner considers it necessary to emphasise that the controller remains responsible for ensuring that its processing operations are compliant with the provisions of the Regulation, irrespective of the payment channel being used. Accordingly, the controller remains fully responsible for ensuring that no more personal data than is strictly necessary is collected from the data subjects using the “*Pay a Bill*” portal, even if there are alternative means by which data subjects can settle bills owed to the controller.
25. After assessing all the circumstances of the case, the Commissioner concluded that the controller failed to effectively demonstrate that the processing of the complainant’s mobile number is necessary for the stated purpose of informing him in the event of an erroneous or suspicious payment being made through the ‘*Pay a Bill*’ portal. The purpose pursued by the controller could have been achieved through less intrusive means, and accordingly, the Commissioner determines that the controller has not acted in compliance with the principle of data minimisation under article 5(1)(c) of the Regulation when it required the collection of the mobile number to enable the complainant to make a bill payment via the ‘*Pay a Bill*’ portal.

On the basis of the foregoing considerations, the Commissioner concludes that the controller failed to effectively demonstrate that the collection of the complainant's mobile number was adequate, relevant, and limited to what is necessary for the purpose of making a bill payment via the 'Pay a Bill' portal on [REDACTED] online banking application. Accordingly, the Commissioner is hereby deciding that the controller infringed the principle of data minimisation under article 5(1)(c) of the Regulation.

In addition, the controller failed to cooperate in a timely manner when requested to provide information necessary for the purpose of enabling the Commissioner to perform his investigative tasks, and therefore, this caused unnecessary delays. Consequently, the controller infringed article 31 of the Regulation.

Pursuant to article 58(2)(b) of the Regulation, the Commissioner is hereby serving the controller with a reprimand and is warning the controller that in the event of repetitive infringements, the Commissioner will take the appropriate corrective action.

In terms of article 58(2)(d) of the Regulation, the Commissioner is hereby ordering the controller to bring its processing operations into compliance with the provisions of the Regulation by modifying the data fields on its payment form on the 'Pay a Bill' portal in a manner that complies with the principle of data minimisation, by either ceasing to request the mobile number entirely, or alternatively, requesting it exclusively on an optional basis.

The controller shall inform the Commissioner, in writing, of the action taken to implement the order within twenty (20) days from the date of service of this decision. Non-compliance with this order shall lead to the imposition of an administrative fine pursuant to article 83(6) of the Regulation.

Ian  
DEGUARA  
(Signature)

Digitally signed  
by Ian DEGUARA  
(Signature)  
Date: 2025.12.04  
09:40:59 +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 (Chapter 586 of the Laws of Malta), any person to whom a legally binding decision of the Commissioner is addressed shall have the right to appeal to the Information and Data Protection Appeals Tribunal within twenty (20) days from the service of the said decision as provided in article 23 thereof.<sup>12</sup>

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*”.

---

<sup>12</sup> Further information on the appeals procedure is available on the IDPC’s portal at the following hyperlink: <https://idpc.org.mt/appeals-tribunal/>