

[REDACTED]

vs

[REDACTED]

## COMPLAINT

1. On the 29<sup>th</sup> July 2024, [REDACTED] (the “**complainant**”) lodged a data protection complaint with the Information and Data Protection Commissioner (the “**Commissioner**”) in terms of article 77(1) of the General Data Protection Regulation<sup>1</sup> (the “**Regulation**”), alleging that [REDACTED] (the “**controller**”) inadvertently sent a copy of her bank account statement to a third party instead of that of her deceased aunt.
  
2. The complainant submitted the following information in connection with her allegation:
  - a. that, on the 12<sup>th</sup> July 2024, the complainant visited one of the branches of the controller to report the demise of her aunt, [REDACTED] and to return her credit card and internet banking key to the controller;
  
  - b. that the complainant requested one of the staff members of the controller to send a copy of the bank account statement of the deceased aunt directly to the notary;
  
  - c. that, after a few days, the notary informed the complainant that she had received an envelope addressed to herself with a copy of the complainant’s personal bank account statement instead of that of her deceased aunt.

---

<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 (General Data Protection Regulation).

**INVESTIGATION**

3. Pursuant to the internal investigative procedure of this Office, the Commissioner sent a copy of the complaint to the controller and provided the controller with the opportunity to make any submissions which it deemed relevant and necessary to defend itself against the allegation raised by the complainant.
4. On the 23<sup>rd</sup> August 2024, the controller submitted the following salient arguments for the Commissioner to consider during the legal analysis of this case:
  - a. that, on the 12<sup>th</sup> July 2024, the complainant called at the [REDACTED] Branch to report the demise of her aunt, [REDACTED], and on the same day, the complainant contacted the controller through its website to contact her since she had forgotten to order a statement to be sent to her notary;
  - b. that the complaint form which was filled in by the data subject quoted ID card number [REDACTED] rather than the actual number of the deceased, [REDACTED];
  - c. that, on the 15<sup>th</sup> July 2024, the [REDACTED] sent an email to the [REDACTED] attaching the request made by the complainant on the website of the controller;
  - d. that the manager at the [REDACTED] Branch contacted the complainant and asked how she can assist her, and the complainant explained that she had previously visited the branch to report the demise of her aunt, but had forgotten to ask the controller to send the statement of her late aunt to her notary;
  - e. that the logs from [REDACTED] revealed that the manager inputted the complainant's account number instead of the one pertaining to the deceased relative of the complainant;
  - f. that, on the 2<sup>nd</sup> August 2024, the manager contacted the complainant to apologise. however, the complainant complained that notwithstanding the fact that she went to the branch in person, handed in the card and the secure key of the deceased to the bank official, the controller had inadvertently sent her bank account statement to the notary;

- g. that the recording of the first time that the bank manager contacted the complainant revealed that at no time was the account number or any other personal details of the deceased communicated during this phone call, and therefore, making it easier for the bank manager to commit the human error of inputting the incorrect account number;
  - h. that although it has been noted that the statement was sent to the notary as indicated by the complainant, and the same notary informed the complainant about the statement, the controller sent a letter to the notary, informing her to destroy the statement, and this is after several attempts to contact her via email; and
  - i. that, during the internal investigation conducted by the controller, it has been confirmed that this data protection incident has occurred due to a human error, and the fact that the ID card number given in the complaint form was incorrect and the fact that no confirmation of the personal details of the deceased were communicated during the phone call, contributed towards such occurrence.
5. The Commissioner provided the complainant with the opportunity to rebut the arguments raised by the controller. On the 30<sup>th</sup> August 2024, the complainant submitted the following counterarguments for the Commissioner to consider:
- a. that the complainant does not agree with the controller that this was purely a case of human error, but it was a case of negligence and unprofessionalism;
  - b. that whilst it is true that the complainant made a mistake in citing the wrong ID card number of her deceased aunt on the site of the controller, however, the complainant did mention that she visited the [REDACTED] branch on the 12<sup>th</sup> July 2024 to report the demise of her aunt and that she needed a statement of her account in the message;
  - c. that the controller could have easily identified the account for which the statement was requested, in particular, since the complainant returned the credit card and the internet banking key of her deceased aunt at the [REDACTED] branch;
  - d. that the controller contacted the complainant following her message on the controller's website, and therefore, the controller could have easily contacted the complainant again to confirm that the ID card number cited in the form was neither of the complainant's nor of the deceased relative;

- e. that, as a result of this, the cashlink and visa cards of the complainant were cancelled and besides the embarrassment and inconvenience of the payments having been rejected repeatedly, the complainant was faced with the inconvenience of having to wait for a new card to be issued and getting used to a new PIN number as well as informing service providers of the change in the card details for on-line/direct debit payment services; and
  - f. that the complainant stated that a mere apology from the controller does not suffice and that compensation for the breach of protection of her data should be awarded as a result of the embarrassment and inconvenience that the complainant had to suffer due to the cancellation of her bank cards.
6. The Commissioner enabled the controller to provide its final submissions in connection with the counterarguments presented by the complainant. On the 9<sup>th</sup> September 2024, the controller contended that it does not believe that there were , or are any risks to the rights and freedoms of the complainant and this for the following two principal reasons:
- a. the statement was sent to the notary who is providing services to the complainant; and
  - b. the notary confirmed, in writing, that the statement has been destroyed.

## LEGAL ANALYSIS AND DECISION

7. The complainant alleged that the controller inadvertently sent a copy of her bank account statement to the notary, instead that of her deceased aunt, and, therefore, the controller infringed the provisions of the Regulation when it disclosed her personal data, including financial data, to a third party. The internal investigation conducted by the controller did indeed confirm that there was a breach of confidentiality:

*“DPU investigated logs from [REDACTED] which revealed that on the day when the data subject visited the branch, the Bank official, [REDACTED] only accessed the profile and accounts of the deceased. However, logs from [REDACTED] revealed that after the data subject was contacted by [REDACTED] the statement retrieved was the one belonging to the data subject. Therefore, proving that the statement sent belonged to the data subject.” [emphasis has been added].*

8. The Commissioner proceeded to assess how the confidentiality breach happened, in particular, to determine whether the incident was a result of a shortcoming in connection with the processes and procedures of the controller. The scope of the investigation was strictly to establish whether the controller infringed any of the provisions of the Regulation, and depending on the outcome of the investigation, to exercise any of the Commissioner's corrective powers in terms of article 58(2) of the Regulation. The Commissioner clarifies that he does not have the power to award damages to the data subjects and in fact, it is the Court that has the competence to award damages to data subjects. This is in accordance with article 30(2) of the Data Protection Act (Cap. 586 of the Laws of Malta), which provides that the data subject may institute an action for damages against the controller by filing a sworn application before the First Hall of the Civil Court.
9. In its submissions, the controller provided a comprehensive explanation in relation to the facts that led to the materialisation of the confidentiality breach, particularly, that “[l]ogs from ██████ revealed that ██████ inputted the data subject's account number instead of the one pertaining to the deceased”. The controller reiterated that this was a human error and the “*fact that the ID number given in the complaint form was incorrect and the fact that no confirmation of the personal details of the deceased were communicated during the phone call, contributed towards such occurrence*”.
10. The European Data Protection Board (the “EDPB”) states that the “*role of human error in personal data breaches has to be highlighted, due to its common appearance. Since these types of breaches can be both intentional and unintentional, it is very hard for the data controllers to identify the vulnerabilities and adopt measures to avoid them*”<sup>2</sup>. The Article 29 Working Party, the predecessor of the EDPB, refers to the intentional or negligent nature of the breach committed by the controller and provides that “*in general, intent includes both knowledge and willfulness in relation to the characteristics of an offence, whereas ‘unintentional’ means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law*”<sup>3</sup>. The Guidelines consider these circumstances as indicative of negligence, “*such as failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to*

---

<sup>2</sup> Guidelines 01/2021 on Example regarding Data Breach Notification, adopted on the 14<sup>th</sup> January 2021.

<sup>3</sup> WP 253, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 adopted on the 3<sup>rd</sup> October 2017.

*apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them) may be indicative of negligence*<sup>4</sup> [emphasis has been added].

11. After assessing the circumstances of the case, and the series of events that led to the error, the Commissioner established that it materialised when the employee inputted the wrong account number in the system, and as a result, generated the wrong bank account statement, which was subsequently sent to the third party. This, therefore, led the Commissioner to conclude that the confidentiality breach derived from an unintentional human error caused by the inattentiveness of the employee, rather than the lack of implementation of the appropriate measures to prevent such incidents pursuant to the requirements set forth in article 25 and 32 of the Regulation. The breach could certainly not be attributable to the complainant in any way.
12. The Commissioner proceeded to assess the mitigating action taken by the controller following the detection of the confidentiality breach. The controller explained that the notary who received the bank account statement of the complainant confirmed in writing, that the data had been destroyed. In his considerations, the Commissioner noted that the notary is a professional individual who is bound by the professional secrecy, and in fact, the notary confirmed in writing that the data had been deleted.

**On the basis of the foregoing considerations, the Commissioner is hereby deciding that, whereas the disclosure of the bank account statement of the complainant to the third party constitutes a confidentiality breach, based on the circumstances of the case, the facts established during the course of the investigation and the mitigation action taken by the controller upon being informed about the matter, the breach was, or is unlikely to result in a risk to the rights and freedoms of the complainant.**

Ian                    Digitally signed  
DEGUARA        by Ian DEGUARA  
(Signature)      (Signature)  
(Signature)      Date: 2024.09.11  
                         11:40:14 +02'00'

**Ian Deguara**  
**Information and Data Protection Commissioner**

---

<sup>4</sup> *ibid.*3.



### 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’*<sup>5</sup>.

---

<sup>5</sup> More details are available here: <https://idpc.org.mt/appeals-tribunal>.