**Information and Data Protection Commissioner**

**CDP/COMP/705/2024**

[redacted]

**vs**

[redacted]

## COMPLAINT

1. On the 14th October 2024, [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[1] (the "**Regulation**"), alleging that [redacted] (the "**controller**" or the "**bank**") infringed the provisions of the Regulation.

2. The complainant explained that he received a 'Commencement of Employment' letter from [redacted] addressed to a third party at his residential address. The complainant further stated that he attended a recent interview at the controller and his address was included in his curriculum vitae which he had submitted as part of a job application. This therefore led the complainant to believe that the controller had mishandled his personal data and erroneously disclosed such data to [redacted] As supporting documentation, the complainant provided the Commissioner with a copy of his identity card document to verify his residential address. Additionally, the complainant supplied a copy of the 'Commencement of Employment' letter received from [redacted] that also contains the same address.

## INVESTIGATION

3. Pursuant to the internal investigative procedure of this Office, the Commissioner provided the controller with a copy of the complaint and enabled the controller to provide any information that it deemed relevant and necessary to defend itself against the allegation raised by the

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

complainant. By means of a letter dated the 12th November 2024, the controller submitted the following salient arguments for the Commissioner to consider during the legal analysis of this case:

a. that following an internal investigation conducted by the controller, it transpired that this was a case of human error;

b. that the employee was recruited to fill in the position of [redacted]' with the controller as from the 1st October 2024;

c. that the HR employee of the controller, who duly registered the employment of the employee in the [redacted] portal, intended to register the employee's address at [redacted], but erroneously chose Naxxar, from the drop-down list, instead of Ta' Xbiex;

d. that it is pure coincidence that the same address in Naxxar pertains to another applicant that applied for a job with the controller;

e. that it is pertinent to state that, unless an applicant is recruited, the HR employee inputting the details in the [redacted] portal does not have access to the applicant's data, and this is because applications for jobs are managed separately by a recruitment officer within the bank; and

f. that in line with the provisions of the Regulation, the controller has informed its employee of the incident and acknowledged the mistake.

4. The Commissioner provided the complainant with the opportunity to rebut the submissions of the controller. By means of an email dated the 21st November 2024, the complainant argued:

a. that, whereas the complainant acknowledges that mistakes may be made, whether intentional or not, individuals and organisations handling personal data are obliged to do so appropriately and pursuant to the applicable data protection law;

b. that the fact that the controller had the residential address of the complainant on file, and that a few months later, he received a letter addressed to another individual at his address for employment purposes indicates a lack of proper control over the personal data processed by the controller;

c. that the explanation provided by the controller in its submissions does not point towards using his exact unique address and the complainant finds it implausible that the entry of his house and street name in the portal of [redacted] system is purely coincidental; and

d. that the complainant requests a proper explanation of the so-called error, including any documentation or logs of the error and how the system would allow for such an error to occur.

5. The Commissioner provided the controller with a copy of the counterarguments of the complainant and enabled the controller to provide its final submissions in relation to this complaint:

a. that a mistake is never intentional, by definition;

b. that the handling of personal data in accordance with the Regulation cannot guarantee that mistakes are never made, and in fact, this was not a systematic error, but a very unfortunate human error, and therefore the controller categorically refutes the statement by the complainant that the incident "... *demonstrates a lack of proper controls over personal data*";

c. that the complainant's address is not in the controller's file, and it never was, and the complainant's address may have been contained in a CV that the complainant may have submitted upon applying to a vacancy however the controller holds no record of that;

d. that whilst the controller understands the perplexity of the complainant stating that it is "*highly unlikely*" that the door number and the street name of the employee match exactly those of the complainant – as already indicated in the previous submissions of the controller – this was in fact the case;

e. that, unfortunately, there is no log to evidence the mistake, and this was simply a case by someone inputting the wrong location in the [redacted] portal, leading to a wrong recipient, incidentally (as much as unlikely), the latter happening to be an unsuccessful applicant to a vacancy of the controller;

f. that, the complainant in this case suffered no damage, other than an inconvenience of receiving an envelope clearly not addressed to him but to the third party – which he unilaterally decided to open;

g. that this is a typical 'snail mail mistake' as contemplated in case no. 13 of the EDPB Guidelines 01/2021 on examples regarding Data Breach Notification; and

h. that the incident only affected the employee's data and not the complainant.

Further clarification sought by the Commissioner

6. The Commissioner requested the controller to provide evidence that the address of the third party is indeed [redacted]. The controller submitted that at the time of recruitment, the employee was living at the address indicated, however, more recently, the employee informed the controller that he changed his residence to a permanent address, and this was duly noted and verified by the controller. The controller confirmed that the file of the employee now contains the updated address.

**LEGAL ANALYSIS AND DECISION**

7. The complainant alleged that the controller erroneously disclosed his residential address to [redacted]. The complainant substantiated his allegation by submitting a copy of the 'Commencement Letter' received from [redacted], which clearly indicated that his residential address was incorrectly linked to an employee of the controller.

8. For the purpose of the investigation of this complaint, the Commissioner proceeded to assess how the incident occurred, in particular, to determine whether the incident was a result of shortcomings in the controller's procedures and processes in relation to the handling of personal data. Consequently, the scope of the investigation was to determine if there is a systematic failure on the part of the controller to ensure the accuracy of the data processed for the purpose of employment and HR purposes.

9. During the course of the investigation, the Commissioner requested the controller to submit any information which it deemed relevant and necessary to defend itself against the allegation raised by the complainant. The controller explained that the incident occurred due to human error and was purely coincidental. The HR employee responsible for registering the employment of the employee intended to input the address at [redacted]. However, the HR

employee mistakenly selected 'Naxxar' from the drop-down list instead of 'Ta' Xbiex'. The complainant expressed incredulity that the controller could make such an error in entering his residential address related to the commencement of the third party's employment. This concern is particularly notable given that the complainant had previously submitted his residential address in his curriculum vitae when applying for a job with the controller.

10. In its submissions, the controller emphasised that unless an applicant has been successfully recruited, the HR employee entering the details into th[redacted] portal does not have access to the personal data of the complainant. This is due to the fact that job applications are handled independently by a designated recruitment officer within the bank. In addition, the controller stated that the address of the complainant was not stored in its files, and therefore, the address of the complainant was not processed in any of the systems of the controller. This therefore led the Commissioner to establish that this is not a case of a controller that is processing inaccurate personal data or mishandling data.

11. The Commissioner considered the Guidelines of the European Data Protection Board (the "**EDPB**"), which 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*"[2].

12. 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***"[3]. 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 apply technical updates in a timely manner, failure to adopt polices (rather than simply failure to apply them) may be indicative of negligence*"[4] [emphasis has been added].

[2] Guidelines 01/2021 on Example regarding Data Breach Notification, adopted on the 14th January 2021.
[3] WP 253, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 adopted on the 3rd October 2017.
[4] ibid.3

13. In the present case, the error stemmed from the incorrect inputting of data into the portal of a [redacted] and failure to check the data before its submissions, which subsequently led to the inaccurate processing of data by JobsPlus, acting as a separate controller. As a result, the Commissioner determined that the incident derived from an unintentional human error caused by the inattentiveness of the employee of the controller, rather than the lack of implementation of the appropriate measures to prevent such incidents pursuant to the requirements set forth in article 24 and 32 of the Regulation.

**On the basis of the foregoing considerations, the Commissioner concludes that the controller submitted incorrect data to the [redacted] portal, and this incident manifested itself as a consequence of a human error stemming from lack of attention exercised by the employee of the controller. This error subsequently led to the inaccurate processing of personal data by a separate controller. The controller is hereby being requested to ensure that [redacted] is notified of any inaccuracies in the data entered by the controller, unless this communication has already been made.**

**Whereas the Commissioner hereby decides that the complainant did not suffer any risks to his fundamental rights and freedoms which warrant the taking of corrective measures against the controller, he nonetheless encourages the controller to ensure that members of staff handling personal data are provided with periodic data protection training. Internal policies and procedures governing the processing of personal data should also be periodically brought to the attention of these employees. A read-and-sign mechanism that they have read and understood the contents of these documents is considered as a best practice approach.**

Ian DEGUARA (Signature)
Digitally signed by Ian DEGUARA (Signature)
Date: 2024.12.16 14:10:31 +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[5].

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*".

[5] Further information is available on the Office's portal at the following hyperlink: https://idpc.org.mt/appeals-tribunal/