Information and Data Protection Commissioner

CDP/COMP/8/2025

[redacted]

vs

[redacted]

COMPLAINT

1. On the 7th of January 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[1] (the "**Regulation**"), alleging that [redacted] (the "**controller**" or [redacted]) improperly handled her FS3 (Statement of Earrings) Form, by sending a copy thereof via email to her, as well as to an unauthorised third party.

2. For the purpose of supporting her allegation, the complainant submitted a copy of the email which demonstrates that the payroll provider engaged by the controller, namely [redacted] (the "**processor**"), sent the FS3 Form on behalf of the controller to both the complainant's email address and to another email address. Notably, the email address was a personal Gmail account that was not associated with either the controller's or the processor's business.

INVESTIGATION

3. Pursuant to the internal investigative procedure of this Office, the controller was provided with a copy of the complaint and was given the opportunity to make any submissions it deemed relevant and necessary to defend itself against the allegation made by the complainant.

4. By means of an email sent on the 30th of January 2025, the controller made the following submissions for the Commissioner to consider in the legal analysis of the present case:

[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.

i. that the controller has an agreement with [redacted] for the provision of payroll services;

ii. that the third party referred to in the complaint, namely the individual whose email address was included in the email containing the complainant's FS3 Form, is an employee of [redacted] and her work tasks and assignments include the payroll services being rendered to the controller;

iii. that it appears the complainant had, prior to this incident, reported to [redacted] that she was having issues receiving her payroll information. Consequently, [redacted] informed the controller that to confirm that there were no issues emanating from [redacted] email address, the employee of [redacted] had included her own email address in copy in that particular communication for testing purposes;

iv. that regrettably, the employee had included her personal email address (a Gmail email address) instead of her professional work email address, which is likely what prompted the complainant's concern, and that this was likely an unfortunate lapse in judgement on the part of [redacted] and its employee, and not the result of any malicious intentions; and

v. that the controller has written to [redacted] requesting confirmation that its employee has: (i) deleted the email, (ii) not forwarded the email to any other individual or account, and (iii) not downloaded the complainant's FS3 Form, or saved it locally, or passed it on, or shared it with anyone. The controller also stated that it will follow up on this, as necessary, and has also required [redacted] to take immediate action and share with it the remedial measures which it will implement to avoid the re-occurrence of any similar incidents in the future.

5. The Commissioner shared the submissions of the controller with the complainant to provide her with the opportunity to respond to and rebut the arguments presented. The complainant did not make any further submissions.

Further Clarification sought by the Commissioner

6. After reviewing the controller's submissions, the Commissioner requested further information from the controller, namely:

i. to clarify the nature of the relationship between [redacted] and [redacted] so as to verify whether [redacted] role is that of a processor vis-à-vis [redacted] and

ii. to provide written confirmation from the employee of [redacted] that said employee has "*(i) deleted the email; (ii) not forwarded the email to any other individual or account; and (iii) not downloaded the Complainant's FS3 Form, or saved it locally, or passed it on, or shared it with anyone*", and of the measures [redacted] intends to implement to prevent the occurrence of any similar incidents in the future.

7. By means of an email dated the 31st of January 2025, the controller submitted that based on its assessment, [redacted] has a controller-processor relationship with [redacted] and that this position was also communicated in [redacted] own privacy notice.

8. In addition, in an email dated the 12th of February 2025, the controller submitted that written confirmation was received from its processor regarding the incident, as follows:

i. as to the cause of the incident – the processor confirmed that a member of its staff, in the process of providing assistance to the controller, used her own email address in the 'CC' field, and that this was done for the purpose of verifying that the email in question arrived successfully at its destination. The processor acknowledged that "*while done in good faith, this approach was not of the required level and could have been done differently*"; and

ii. as to the remedial measures taken – the processor confirmed that "*the email in question has since been deleted and no record remains of this email outside of* [redacted] *official records*", and that in the event of similar tests being required in the future, only the email addresses of the relevant persons requiring access will be considered.

LEGAL ANALYSIS AND DECISION

The Role of the Controller and the Processor

9. In order to understand their respective roles in relation to the processing of personal data, the Commissioner assessed the nature of the relationship between [redacted] and [redacted] explained that it has a contractual agreement with [redacted], in terms of which, [redacted] is

engaged to administer the payroll to the employees of [redacted] and in so doing, acts as the processor on its behalf.

10. Upon an analysis of the provisions of the Regulation, article 28(3)(a) clearly requires that the contract entered into between the controller and the processor "*shall stipulate, in particular, that the processor processes the personal data* ***only on documented instructions from the controller***". As part of his legal analysis, the Commissioner proceeded to analyse the European Data Protection Board ("**EDPB**") **Guidelines 07/2020 on** the Concepts of Controller and Processor in the GDPR **which state that,** "*processors must always comply with, and act only on, instructions from the controller*". Yet, "***the controller's instructions may still leave a certain degree of discretion about how to best serve the controller's interests*** *[...]*"[2] [emphasis has been added].

11. In this regard, the Guidelines 07/2020 acknowledge that while the controller always determines **the purposes and essential means of processing,** "*some more practical aspects of implementation ("****non-essential means****") can be left to the processor.*"[3] Hence, processors enjoy a limited degree of discretion in the practical performance of their tasks. However, this degree of leeway should be exercised with caution, to avoid scenarios where an action which may not have been contemplated in the agreement between the controller and the processor, or which was not directly authorised by the controller, may give rise to an infringement of the Regulation.

12. In the present case, the personal data breach occurred when the processor, while acting to serve the controller's interests, **decided to conduct an internal test to confirm that the emails being** sent out by the processor to the employees of the controller were being successfully delivered.

13. In this regard, and in accordance with the requirements of article 24 of the Regulation and the principle of [redacted]ability, the Guidelines stress that it is "***the controller [that] remains responsible for the implementation of appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is performed in accordance with the Regulation***"[4], and therefore, the controller must be fully informed about the means that are used, so that it can take its own informed decision on those means.

---

[2] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, adopted on the 7th July 2021, paragraphs 9 and 80.
[3] Ibid. p. 3.
[4] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, adopted on the 7th July 2021, paragraph 41.

14. In her complaint, the complainant alleged that the controller had improperly handled her FS3 Form, because the form was sent not only to her email address but also to the email address of a third party. The complainant substantiated her allegation by submitting a copy of the email sent by the processor, which clearly demonstrated that the Form was transmitted to the complainant's email address as well as to another '*Gmail*' address which did not appear to be a company email address that was connected to the controller or the processor.

15. For the purpose of investigating the complaint, the Commissioner sought to establish how the incident occurred, to determine whether the confidentiality breach resulted from any inherent shortcomings or deficiencies in the controller's procedures and processes for the handling of personal data. Consequently, the scope of the investigation was to identify whether there was a systematic failure on the part of the controller to ensure the secure handling of employee personal data that is communicated via email.

16. During the course of the investigation, the Commissioner had requested the controller to clarify whether the third party individual's access to the complainant's personal data was justified and if so, on what grounds – particularly given that the complainant's personal data was sent to a personal Gmail account and not to an official company email address. In response, the controller provided a comprehensive explanation, stating that the individual was an employee of the processor, and acknowledged that the inclusion of the employee's personal email address as a recipient had likely resulted from "*an unfortunate lapse in judgement on the part of* [redacted] [the processor] *and their employee.*"

17. As part of his legal analysis, the Commissioner examined the role that human error can play in the context of personal data breaches, which the EDPB recognises as being a common and frequently occurring issue. In particular, the Commissioner analysed the EDPB Guidelines 01/2021 on Examples Regarding Personal Data Breach Notification, which state 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*"[5].

[5] EDPB Guidelines 01/2021 on Examples regarding Data Breach Notification, adopted on the 14th January 2021, paragraph 71.

18. Furthermore, in its Guidelines, the Article 29 Working Party (the predecessor of the EDPB) specifically refers to and distinguishes between infringements of an intentional character and infringements of a negligent character,[6] stating that, "*in general, "intent" includes both knowledge and wilfulness 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***" [emphasis has been added]. In particular, the Article 29 Working Party Guidelines cite "*human error*" as a specific example of a circumstance that may be indicative of negligence.

19. In the present case, the confidentiality breach occurred when the processor, while acting on behalf of the controller to send out payroll information to the controller's employees, carried out an internal test to confirm the successful delivery of the emails being sent out by the processor. In so doing, the processor's employee sought to include herself as a recipient of the email, and had included her personal email address instead of her professional one. According to the statement given by the processor, this was done in good faith, and devoid of any malicious intent.

20. After assessing all the circumstances of the case, the Commissioner considered that the breach derived from an unintentional – albeit still negligent – act of human error on the part of the processor's employee, rather than due to a lack of implementation of the appropriate measures to prevent such incidents and ensure the security of processing pursuant to the requirements of article 32 of the Regulation. Additionally, the Commissioner also considered that other than the intended recipient, the email was sent only to one other individual, who was part of the organisation and who took immediate action to delete the email.

21. Finally, the Commissioner also considered the remedial action taken by the controller following the breach to mitigate the possible adverse effects to the complainant. The controller had obtained written assurance from the processor that the employee had permanently deleted the email, and that no copies of the email exist outside of the controller's official records. Furthermore, the processor gave its assurance that if similar tests need to be carried out in the future to verify the successful delivery of the processor's emails, only the email addresses of those individuals within the organisation who strictly require access will be included.

[6] Article 29 Working Party 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.

On the basis of the foregoing considerations, the Commissioner is hereby deciding that, whereas the transmission of the complainant's FS3 Form to the personal email address of the processor's employee constitutes a breach of confidentiality, based on the circumstances of the case, the facts established during the investigation, and the mitigating action taken by the controller, the breach was, or is, not likely to result in a risk to the rights and freedoms of the complainant.

Ian DEGUARA (Signature)

Digitally signed by Ian DEGUARA (Signature)
Date: 2025.02.24 12:17:00 +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.[7]

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*".

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