

Information and Data Protection Commissioner

CDP/COMP/130/2025

vs

COMPLAINT

1. On the 6th March 2025, Ms [REDACTED] ("**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 Regulation¹ (the "**Regulation**"), alleging that [REDACTED]² which was subsequently struck off following a merger with [REDACTED]³ (the "**controller**"), unlawfully accessed and processed her personal data on her personal device, as well as failed to comply with her subject access request (the "**SAR**").

INVESTIGATION

2. Following receipt of the complaint, the Commissioner began investigating the complainant's allegation that the controller had unlawfully accessed and processed her personal data. After preliminarily assessing the admissibility of that allegation, the Commissioner proceeded to preliminarily assess the complainant's further allegation that the controller had not complied with her SAR.

Background of the complaint

3. The complainant elaborated on the following pertinent matters, as part of her complaint:

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 (General Data Protection Regulation).

² Bearing Malta company registration number C [REDACTED]

³ Bearing Malta company registration number C [REDACTED]

- a. that the controller had lost her original personal laptop during an office move and, consequently, provided her with a substitute laptop as a replacement which, whilst remaining as her personal laptop, was “*configured by [the controller’s] IT contractor... during [her] employment*”;
- b. that the controller “*accessed, copied, processed and misused*” her personal data without “*lawful reason*”, allegedly in the context of having “*received Microsoft security notifications via email ... showing multiple unauthorised login attempts*”; and
- c. that the controller failed to duly fulfil her SAR.

Information sought from the complainant

4. In connection with the contention of failure to comply with the complainant’s SAR, the Commissioner requested that the emails mentioned in her complaint, dated the 20th and 24th February 2025, be forwarded for his perusal, including any response which she may have received in the interim.
5. By means of an email dated the 10th December 2025, the complainant provided the emails requested, along with the following pertinent annotations:

“Email from [complainant] to the controller [REDACTED] dated 20 February 2025. Endeavor responded to this email on 21 February 2025...”

Email from [complainant] to [REDACTED] dated 24 February 2025, to which they have never responded directly...”

6. By means of a response to the complainant by email that same day, the Commissioner requested the complainant to therefore confirm the understanding, that no reply in the interim had been received on the SAR, from the controller.
7. As no response had been received from the complainant, the Commissioner followed up by means of email on the 16th December 2025, requesting a copy of the SAR submitted to the controller by email dated the 14th February 2025.
8. By means of an email from the complainant that same day, a copy of the SAR file(s) provided by the controller to the complainant on the 14th March 2025, were forwarded to the Commissioner, along with the following remarks by the complainant:

- a. that *“the information supplied was very limited, with only a small portion of the communications included, and they did not properly address the scope of my SAR request of 14 February 2025”*; and
 - b. that *“[i]n addition to the information shared via the link above, their response also included my Clockify time tracking file and leave history, and nothing further”*.
9. In view of the complainant’s submissions, the Commissioner requested the complainant by means of an email dated the 19th December 2025, to indicate to the Commissioner what personal data she believed, were missing from the SAR file shared by the controller.
 10. As no response had been received from the complainant, the Commissioner followed up with the complainant by means of an email dated the 22nd December 2025, which moreover emphasised the request to list clearly, the personal data claimed to be missing, by the former.
 11. By means of an email dated the 23rd December 2025, the complainant provided a list of the personal data and communications, she contended were missing from the SAR file provided by the controller.

Request for submissions

12. By means of an email dated the 5th January 2026, and pursuant to the internal investigative procedure of this Office, the Commissioner provided the controller with a copy of the complaint, including the supporting documentation, and enabled the controller to submit any information that it deemed necessary and relevant to defend itself against the allegation raised by the complainant.
13. As no response was forthcoming, a final letter and opportunity dated the 30th January 2026 was issued to the controller via post, for their submissions in relation to the complaint.

Submissions of the controller

14. On the 16th February 2026, the controller confirmed receipt of acknowledgement of the Commissioner’s letter and confirmed that it had been received on the 11th February 2026.
15. By means of an email dated the 20th February 2026, the controller provided the Commissioner with a letter comprising of its submissions, for the Commissioner to consider during the legal

analysis of the case. The controller submitted the following salient arguments:

The controller's internal policy following a termination of employment

- a. that the controller does not maintain at present a written internal policy, specifically documenting post-termination procedures, yet this is something that the controller is working on formally documenting;
- b. that the procedure taken with respect to the complainant's termination of employment is the "*standard Company procedure*", and applicable upon termination of any and all of the controller's employees;
- c. that, upon the complainant's termination of employment, "*the [controller's] IT service provider promptly locked the [c]omplainant's corporate account and revoked her access to the [controller's] systems including access to her work email...*" including access to other company-related services;

The status of the laptop in the course of the complainant's work

- d. that the laptop in question is the complainant's personal property, which the controller had agreed to purchase for the complainant as a replacement of the complainant's prior personal laptop which was misplaced and lost in the course of the company's office move;
- e. that, such laptop, despite being the complainant's personal property, was being used by her for work purposes to perform her employment duties;
- f. that the controller provided the complainant with a corporate account for her to be able to access the controller's IT systems, through the laptop in question;

Ability or otherwise to remotely access the laptop

- g. that, whilst it was confirmed that the controller, through its processors, and the processors acting on behalf of the controller, had and do have the ability to remotely access the complainant's personal laptop, remote access to the complainant's laptop, during her period of employment, "*was made with the [c]omplainant's knowledge and awareness, and exclusively for legitimate purposes such as resolving IT issues or installing software upgrades...*";
- h. that, following the complainant's termination of employment, her corporate account was locked as part of "*the [controller's] standard security protocol to prevent the*

[c]omplainant's continued access to the [controller's] data and systems";

- i. that, "as a consequence, although in theory the [controller] and its processors do have the ability to remotely access the [c]omplainant's laptop, for this to be done, the laptop would need to be switched on, connected to the internet and logged into the account" and moreover that, "[g]iven that the [c]omplainant cannot use the laptop due to the fact that her corporate account has been locked by our processors, then it goes without saying that neither the [controller] nor the processors acting on behalf of the [controller], can log in to her account remotely";
- j. that, "[i]n any case, even if the [controller] or its processors had remotely logged in to the [c]omplainant's account, the [c]omplainant would notice and be aware that such logging in had been done";

The access attempts referred to by the complainant

- k. that "neither the [controller] nor its processors were responsible for, or involved in, the access attempts" forwarded by the complainant towards the end of February 2025; and

Subject Access Request (SAR)

- l. that in relation to the complainant's allegation that her SAR of the 14th February 2025 was only partially complied with by the controller, "the [controller] respectfully submits that it complied with the SAR to the fullest extent possible" and that "[t]he [controller] confirms that it has provided the [c]omplainant with a copy of all her personal data undergoing processing by the [controller]".

Counterarguments of the complainant

- 16. As part of this Office's internal investigative procedure, the Commissioner provided the complainant with a copy of the submissions provided by the controller and enabled the complainant to submit her counterarguments.
- 17. By means of an email dated the 4th May 2026, the complainant made her counterarguments for the Commissioner to consider during the legal analysis of the case. The complainant provided the following salient arguments:
 - a. that the controller submitted that it complied with the complainant's SAR to the fullest extent possible and provided all her personal data undergoing processing – that this is not correct; and

- b. that they provided very limited information in response to the SAR, lacking access to important emails, information and personal data.

LEGAL ANALYSIS AND DECISION

18. For the purpose of this legal analysis, the Commissioner proceeded to examine the subject-matter of the complaint, in which the complainant alleged that the controller failed to comply with the complainant's SAR request and unlawfully processed her personal data through the alleged unauthorised remote access to her laptop.

Allegation in relation to unlawful processing

19. The Commissioner notes that the complainant is a former employee of the controller, and that the laptop in question was purchased by the controller during her employment following the misplacement of her previous personal laptop during an office move.
20. The complainant specified that the laptop, which had been purchased by the controller as a replacement, was "*configured by [the controller's] IT contractor*" during her employment.
21. The Commissioner also notes the controller's submissions that "*such laptop was also being used by the [c]omplainant for work purposes to perform her employment duties. In this respect, the [controller] provided the [c]omplainant with a corporate account for her to be able to access the [controller's] IT systems through the laptop*".
22. That this configuration was done for "*legitimate purposes such as resolving IT issues or installing software upgrades and upgrades*".
23. The Commissioner notes, that the foregoing can be witnessed in industry practice, in the event for instance of contract breach or termination of employment, such as in the case at hand. Accordingly, the controller submitted that "*[u]pon the [c]omplainant's termination of employment, the [controller's] IT service provider promptly locked the [c]omplainant's corporate account and revoked her access to the [controller's] systems including access to her emails...*".
24. The complainant requested the Commissioner to restore sign-in access to her laptop after the controller locked her account and revoked her access to its systems. From the controller's submissions, the Commissioner further notes that these measures were implemented in

accordance with the controller's "*standard security protocol*"⁴.

25. The Commissioner points out that the scope of the Regulation relates to the protection of processing of personal data, by automated means or in the context of a filing system⁵. Accordingly, the Commissioner will not enter into the merits of account sign-in access or otherwise, as this is beyond the scope of the Regulation and the Commissioner's powers thereunder.
26. For this reason, the Commissioner proceeded to examine the complainant's allegation that the controller unlawfully processed her personal data through the alleged unauthorised access to her personal computer.
27. The Commissioner notes the complainant based the foregoing allegation on Microsoft security notifications received by email indicating login attempts on the 24th, 25th and 26th February 2025. The complainant alleged that these login attempts occurred in close proximity to the controller restricting her access to the account following the termination of her employment.
28. The Commissioner proceeded to evaluate this allegation in light of the supporting documentation provided by the complainant and sought the controller's submissions on this allegation, including in the context of the referred Microsoft sign-in attempts⁶ – along with the contention of failure to comply with the SAR of the complainant.
29. The Commissioner notes the controller's arguments that, whilst the controller, through its processors had (and do have) the ability to remotely access the complainant's personal laptop, remote access was carried out during the complainant's period of employment and was made with her knowledge and awareness, for "*resolving IT issues or installing software upgrades and upgrades*". The controller moreover affirmed that "*neither the [controller] nor its processors were responsible for, or involved in, the access attempts*" highlighted by the complainant, on the 24th, 25th and 26th February 2025⁷.
30. The Commissioner further notes the controller's arguments that, following the complainant's termination of employment, its IT service provider locked the complainant's corporate account and revoked her access to the controller's systems, including access to her work email,⁸ in

⁴ Vide paragraph 15.h hereof.

⁵ Article 2(1) of the Regulation.

⁶ Vide Paragraph 3.b hereof.

⁷ Vide Paragraph 15.k hereof.

⁸ Vide Paragraph 15.c hereof.

pursuance of the controller's standard security protocol.⁹

31. Consequently, the controller stressed that, although in theory the controller and its processors do have the ability to remotely access the complainant's laptop, *"for this to be done, the laptop would need to be switched on, connected to the internet and logged into the account"*¹⁰. Accordingly, the controller submitted, that *"[g]iven that the [c]omplainant cannot use the laptop due to the fact that her corporate account has been locked by [the controller's] processors, then it goes without saying that neither the [controller] nor the processors acting on behalf of the [controller], can log in to her account remotely"*.¹¹

32. In view of the foregoing, the Commissioner notes there is a lack of sufficient evidence to support the claim that the controller remotely accessed and processed the complainant's personal data through her laptop in the manner alleged by the complainant.

SAR

33. The Commissioner proceeded to examine the complainant's contention that the controller did not comply with her SAR.

34. As a point of departure, the Commissioner notes that the controller responded to the complainant's SAR of 14th February 2025 within one (1) month from the date she exercised such request.¹²

35. The Commissioner considered article 15(3) of the Regulation which imposes on the controller the obligation, upon request, to provide a copy of the *"personal data undergoing processing"*.

36. The Commissioner further considers that the notions of *"personal data"* and *"processing"* are to be read in light of the material scope of the Regulation which extends its application to the processing of personal data by automated means and to the processing other than by automated means of personal data which form part of a filing system and prescribes certain activities as falling outside of the Regulation's scope.

37. The Regulation therefore acknowledges that, not all activities of processing of personal data

⁹ Vide Paragraph 15.h hereof.

¹⁰ Vide Paragraph 15.i hereof.

¹¹ Vide Paragraph 15.i hereof.

¹² Paragraph 8 hereof.

necessarily fall under the applicable scope of the Regulation.

38. Pursuant to investigating the SAR contention of the complaint, the Commissioner notes from the complainant's submissions that the controller's response contained a copy of personal data relating to her, pursuant to her SAR. The Commissioner accordingly requested the complainant to forward the SAR file provided by the controller.
39. The Commissioner proceeded to peruse the SAR file provided, in conjunction with the complainant's contention that "[t]he information supplied [in the SAR response] was very limited, ..." and that "they did not properly address the scope of [her] SAR request..."¹³.
40. In view of the allegation of missing/incomplete personal data, the Commissioner requested the complainant to detail which personal data referred to she believed were missing from the SAR file forwarded by the controller on the 14th March 2025.
41. Following the complainant's response detailing the personal data excerpts she believed to be missing, the Commissioner pursued its investigation in this respect with the controller.
42. After analysing the underlying email communications in question, the Commissioner confirmed that the emails in question were exchanged by the complainant in her capacity as an employee during her employment with the controller.
43. The inherent nature and purpose of emails exchanged by an employee by means of a corporate email account, which is a tool that an employer provides to the employee to carry out certain employment duties, implies that those emails are not intended to be used for private or personal purposes. 
44. Electronic communications sent by an employee through their corporate email in the context of work are considered to be sent on behalf or in the name of the employing organisation. It is not disputed that a corporate email address in the format name.surname@company.com constitutes 'personal data' within the meaning of article 4(1) of the Regulation, though the content of such mail itself, may not necessarily involve personal data relating to the individual in question.
45. The above-described predisposition of business affairs – absent of personal ties – is incidentally reflected in the Regulation's scope of rights and safeguards, which is extended to

¹³ Paragraph 8.a hereof.

private citizens and *not* legal persons or entities.¹⁴

46. Notwithstanding any sanctioning by employers in governing the use of corporate accounts by employees, employees may still decide to use such corporate accounts for non-work-related purposes and hence inadvertently include information of a private or personal nature.
47. Insofar as this kind of information is concerned, employees filing a right of access request with their current or former employer, have the right to obtain a copy of such communications which, due to their inherent personal nature, constitute personal data within the definition of the Regulation. Emails however sent from a corporate email account containing business or client related information, and hence in pursuit of their organisation's mandate/duties, fall outside the prerogative to exercise a right of access under the Regulation, for the above considered reasons.
48. Following the Commissioner's investigation on the complaint that the controller failed to fulfil the complainant's SAR, the Commissioner concluded that the controller's SAR response with the complainant's personal data, on 14th March 2025, was in conformity with article 15 of the Regulation.

DECISION

In view of the foregoing considerations, the Commissioner hereby dismisses the complaint in its entirety, on the basis that information gathered during the course of the investigation did not yield conclusive evidence that the controller unlawfully processed the complainant's personal data, and confirmed that the controller fulfilled the complainant's right of access request in accordance with the Regulation.



Dr Reno Borg

Information and Data Protection Commissioner

Decided today, 5th August 2026

¹⁴ Recital 14 of the Regulation.

Right of Appeal

The parties are hereby being informed that in terms of article 26(l) 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 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.¹⁵

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*".

¹⁵ Further information is available on <https://idpc.org.mt/appeals-tribunal/>.