Information and Data Protection Commissioner

CDP/COMP/280/2023

[redacted]

vs

[redacted]

COMPLAINT

1. On the 1st March 2023, [redacted] (the **"complainant"**) lodged a 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 a lecturer working for [redacted] (the **"controller"** or the "[redacted]") continued to send Microsoft Teams' links and classwork on her personal email address, without using the *'blind carbon copy'*, and as a result, disclosed her email address to unauthorised third parties.

INVESTIGATION

Request for submissions

2. Pursuant to article 58(1)(a) of the Regulation, the Commissioner provided [redacted] with a copy of the complaint, including the documentation attached thereto, and requested it to put forward its submissions in order to defend itself against the allegations raised by the complainant. By means of an email dated 12th April 2023, [redacted] submitted the following principal arguments for the Commissioner to consider in his legal analysis of the 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 (General Data Protection Regulation).

i. that in an email dated 28th February 2023 sent to the controller, the complainant noted that she had two lectures, one on Monday and the other on Wednesday, during which the lecturer teaching her on Wednesdays consistently sent personal emails, including all other group colleagues in *'CC'*. The complainant expressed her concern that this practice amounted to a data breach, stating that there should be a method to send Microsoft Teams' links and information without divulging personal email addresses;

ii. that on the same day, the complainant sent another email to [redacted]'s general email address [redacted], wherein she informed [redacted] that *"Non-[redacted] users are now using this as a thread with all in copy to my personal email. I did not consent for my personal details to be used in this way. Can this practice please be reviewed?"*. Moreover, in this email, she attached a list of her colleagues' emails as evidence to substantiate her claim;

iii. that the complainant also attached a reply (dated 22nd February 2023) that she received from her lecturer on this subject, stating that *"I am very sorry but the way we send communication is as a group. Kindly send email that we can use in the group to [redacted] admin explaining the situation"*;

iv. that the complainant's lecturer a part-timer at [redacted], with an eight-week contract to teach [redacted], and she admitted to being fully aware of the [redacted]' Data Protection Policy & Procedure;

v. that the lecturer confirmed the following points:

- that the complainant, along with all other class colleagues, were informed prior to their registration for the course that Microsoft Teams served as the designated learning-teaching platform;

- that the lecturer requested the complainant to provide an alternative email, she failed to do so;

- that Microsoft Teams was the designated platform for this module, which was adopted during the Covid era when learning shifted from face-to-face to online, and therefore all the participants' emails were required for communication purposes. Technically, the system could not be altered or modified as it

constitutes an integral part of Microsoft Teams. It was further noted that the Director for Student Services also corroborated all the aforementioned testimonies.

3. In line with the Commissioner's complaint-handling procedure, on the 19th April 2023, the Commissioner provided the complainant with the opportunity to rebut the arguments made by the controller. On the same day, the complainant rebutted the arguments made by the controller and submitted the following salient points:

   i. that the complainant upheld that *"[m]y complaint isn't about teams as I log in with the email provided by* [redacted]*"*;

   ii. that *"[m]y complaint is the fact that lecture material was distributed via my personal email through cc. I had requested bcc as I didn't want my email shared with the people on the course, and it was not just limited to my group"*.

LEGAL ANALYSIS AND DECISION

4. During the course of the investigation, the Commissioner established that [redacted]'s lecturer sent various school-related emails to various recipients using the *'to'* field instead of the *'blind carbon copy'* field. The complainant's personal email address was included in this communication and, as a result, disclosed to the other recipients.

5. The Commissioner notes that an email address which contains the name and surname[2] of a natural personal constitutes "*personal data*" within the meaning of article 4(1)[3] of the Regulation. In this context, recital 26 of the Regulation states that a person may still be identifiable after taking into account "*all the means reasonably likely to be used, such* ***as singling out****, either by the controller or by another person* ***to identify the natural person directly or indirectly****"* [emphasis has been added].

[2] This has been confirmed by the Court of Appeal in Doreen Camilleri vs Kummissarju ghall-Informazzjoni u l-Protezzjoni tad-Data, Appeal No. 63/17.

[3] Article 4(1) of the Regulation defines 'personal data' as *'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;'*

6. Accordingly, the controller is obliged to ensure that its processing activities are carried out in a manner that ensure appropriate security of the personal data, including protection against unauthorised disclosure of, or access to, personal data. By virtue of the principle of accountability held under article 5(2) of the Regulation, the controller is responsible for, and must be able to demonstrate compliance with the principles of data processing, specifically the principle of integrity and confidentiality pursuant to article 5(1)(f) thereof.

7. The principle of integrity and confidentiality is further reflected in article 32(1) of the Regulation, which is more prescriptive and sets out the obligations to which the controller is subject, in terms of data security. In this respect, article 32(1) of the Regulation obliges the controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

8. The Commissioner stresses that the controller should select the appropriate security measures which are necessary to effectively protect the personal data prior to the processing activity. This, therefore, obliges the controller to put in place proactive measures to ensure compliance with the provisions of the Regulation.

9. The obligation of personal data security should therefore be construed as an obligation to guarantee a "*level of security appropriate to the risk*". In this aspect, article 32(2) of the Regulation stipulates that "*in assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed*".

10. After thoroughly examining the submissions furnished by the controller, particularly those presented on the 12th April 2023, wherein it was stated that, *"I am very sorry but the way we send communication is as a group"*, and taking into account the surrounding circumstances that led to the unauthorised disclosure of the complainant's personal data, the Commissioner determined that the controller did not adequately prove that it had implemented the appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

In light of the foregoing, the Commissioner hereby decides that the controller infringed article 32(1)(b) of the Regulation, when it failed to implement the appropriate technical and organisational measures to ensure the ongoing confidentiality of the complainant's personal data, including the principle of integrity and confidentiality pursuant to article 5(1)(f) of the Regulation.

In terms of article 58(2)(d) of the Regulation, the controller is hereby being ordered to implement the appropriate technical and organisational measures to ensure the ongoing confidentiality of the processing of personal data when sending bulk emails to multiple recipients.

Furthermore, the controller is being advised that school-related emails should be sent to the email address provided by [redacted], unless the controller obtains written consent, by virtue of which they assent to the use of their private email for such purposes.

Ian DEGUARA (Signature)
Digitally signed by Ian DEGUARA (Signature)
Date: 2023.07.24 13:05:59 +02'00'

Ian Deguara
Information and Data Protection Commissioner

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.