

[REDACTED]

vs

[REDACTED]

COMPLAINT

1. On the 25th June 2024, Ms [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 Regulation¹ (the “**Regulation**”), alleging that the [REDACTED] [REDACTED] (the “**controller**”) sent a newsletter email, revealing the complainant’s email address with forty-six (46) other recipients.

INVESTIGATION

Request for submissions

2. Pursuant to article 58(1)(a) of the Regulation, the Commissioner provided the controller 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 20th September 2024, the controller submitted the following principal arguments for the Commissioner to consider in his legal analysis of the case:
 - i. that the controller acknowledges that recipients were mistakenly included in the "CC" field instead of "BCC" as a result of a human error;

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).

- ii. that the disclosed data involved was simply her email addresses and the controller has apologised to the complainant regarding the incident;
- iii. that, following an internal risk assessment, after considering the likelihood and severity of risk to data subjects' rights and freedoms, the controller concluded that the incident does not merit a notification of breach;
- iv. that, according to EDPB Guidelines 9/2022, disclosing an individual's name and address under ordinary circumstances is unlikely to cause substantial damage, and in this case no home address was disclosed;
- v. That there is no evidence that any inconvenience occurred, resulting in no meaningful or tangible impact on the complainant, and consequently, the incident was not a notifiable breach.

LEGAL ANALYSIS AND DECISION

3. During the course of the investigation, the Commissioner determined that the controller sent an email with commercial content on the 23rd of June 2023, to multiple recipients using the 'CC' field instead of the 'BCC' field. The complainant's personal email address was included in this communication and, as a result, disclosed to the approximately forty-six (46) recipients.
4. The Commissioner examined article 4(1) of the Regulation which defines "*personal data*" as "*any information relating to an identified or identifiable natural person ('data subject')*". An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier like a name, identification number, or location data, or to one or more factors specific to a person's physical, physiological, mental, economic, cultural, or social identity.
5. The Commissioner notes that an email address which contains the name and surname² of a natural person 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*

² This has been confirmed by the Court of Appeal in '*Doreen Camilleri vs Kummissarju għall-Infommazzjoni u l-Protezzjoni tad-Data*' (Appeal No. 63/17), decided on the 5th October 2018.

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;*

singling out, either by the controller or by another person to identify the natural person directly or indirectly” [emphasis has been added].

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. Following an analysis of the submissions provided by the controller and the circumstances of the case leading to the unauthorised disclosure of the complainant’s personal data, the Commissioner concludes that controller failed to effectively demonstrate that it had taken 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.

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.

After considering the nature of the infringement, the controller is hereby being served with a reprimand pursuant to article 58(2)(b) of the Regulation and warned that, in the event of a further similar infringement, the appropriate corrective action shall be taken accordingly.

Ian
DEGUARA
(Signature)

Digitally signed
by Ian DEGUARA
(Signature)
Date: 2024.10.09
10:18:01 +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'.

