

- i. that in accordance with the controller's corporate procedure, the communication is in line with its legal obligations arising from Regulation. Typically, commercial communications that are intended for multiple recipients, are sent in a manner that ensures recipients do not have visibility into other recipients' email addresses, employing the Blind Carbon Copy (the "BCC") function. However, in this case, the communication was erroneously sent with the use of the Carbon Copy function (the "CC"), allowing recipients to see each other's email addresses due to an oversight;
- ii. that upon realisation that the wrong function had been used for sending the email in question (**marked and annexed as Doc IDPC 1**), the sender used the recall function. The mentioned mistake and the corrective measure of recalling the email were explained to the complainant during her initial communication with the sender;
- iii. that the controller has its privacy notice³ available on its website to inform data subjects regarding data processing activities involving their data. The privacy notice includes, *inter alia*, the contact details that can be used for addressing any personal data related queries. The link to the website, containing the informative privacy notice, is also added to the employees' corporate signatures under their email addresses. Through this policy, the controller aims to make its intentions public and transparent, ensuring accessibility to all data subjects whose personal data is or will be processed;
- iv. that upon its occurrence, the incident was escalated to the director and evaluated at management level. It was determined that the only information visible to unauthorised persons was the '*email address*'. Although this was considered a breach, it was also concluded that it was unlikely to pose a risk to the rights and freedoms of the individuals involved;
- v. that it is also pertinent to note that a simple Google search of complainant's name reveals her current employment and position. Furthermore, "*anyone knowing the naming convention of the company she is employed with can easily arrive at her email address*"; and
- vi. that by acknowledging the importance of personal data privacy, the employee involved was advised to treat personal data more carefully to prevent similar incidents in the

³ [REDACTED] 'Privacy Policy', available at: [REDACTED] [last accessed on the 6th February 2024].

future. Going forward, the controller outlined that it is also revising its manual processes that are prone to human error to enhance accountability and traceability and to provide training to staff.

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 24th October 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 one hundred and eighty (180) 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 surname⁴ of a natural person constitutes "*personal data*" within the meaning of article 4(1)⁵ 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].
6. The Commissioner analysed recital 14 of the Regulation stating that the Regulation does not cover the processing of data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person. However, the publication of the personal email address of a technical contact person consisting of name.surname@company.com can reveal information regarding

⁴ 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.

⁵ 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;*'

their current employer, his or her respective role within the organisation and the individual's place of work.

7. 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.
8. 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.
9. 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.
10. 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”*.
11. 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.

When using an email client or any other similar application, if technically possible, the Commissioner strongly recommends activating and configuring a delay rule wherein the email resides temporarily for the set timeframe in the outbox folder and in the event of a human mistake or error, the email remains accessible for any necessary amendments or changes to be made accordingly.

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: 2024.02.06
16:13:51 +01'00'

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’.