

This is a summary of the decision of the Commissioner.

The Data Protection Office received a complaint from Complainant (Mr X) against Respondents (Companies A and B) alleging that:

When the invitation for a meeting of the shareholders of Company A was sent, the administrator inadvertently addressed the email to all shareholders collectively. The email should have been addressed individually to each shareholder.

Following the statement provided by Mr. X, the DPO wrote to Companies A and B outlining the lawful obligations under the Data Protection Act that the company is required to comply with, as well as the measures to be implemented. The company was also requested to provide further statements on the following:

- i. provide your explanation regarding the complaint;
- ii. What measures and actions have been taken to prevent such incident from occurring; and
- iii. the measures taken at the level of Company to minimize the potential risks to personal data.

The DPO received the replies of Companies A and B, wherein it was mentioned that Company B, acting as the Controller for Company A, acknowledged its responsibilities under the Data Protection Act and confirmed that the data breach on 5 September 2024 was unintentional. The incident occurred when an employee sent an email to all investors of Company A on 29 August 2024, revealing their email addresses and, in some cases, personal data such as names and surnames. The breach was reported to the Data Protection Office on 4 September 2024 and internal procedures were followed.

To prevent recurrence, Company B implemented corrective measures, including using the BCC field for group emails, enforcing a four-eye review policy for outgoing investor communications, and conducting refresher training for all staff on data protection best practices and awareness.

By way of a letter, this Office informed Mr. X of the additional declarations made by Companies A and B and requested him to indicate whether he is satisfied with the measures implemented to remedy the unlawful disclosure of personal data or if he wished to provide any further views.

Subsequently, Mr X was informed on the reply of Companies A and B based on the enquiry conducted, it is observed that:

- a. The company, in its capacity as Controller for Company A, acknowledges its responsibilities under the Data Protection Act.
- b. At Company B, data protection is prioritised through a comprehensive policy applied diligently in daily operations.

Companies A and B inform the Commission that they are satisfied with the measures implemented and have no further comments on the matter.

The Data Protection Commissioner has decided as follows:-

In view of the above, the enquiry has not disclosed the commission of an offence under the DPA and is closed to the satisfaction of all parties under section 6 of the Data Protection Act (DPA).