This is a summary of the decision of the Commissioner.

The Data Protection Office received a complaint from Complainant (ex-employee of Respondent) against Respondent. In her declaration, Complainant stated that:

1. She has just realised that another person had accessed her Dropbox(under her personal email address) documents which are still linked in her ex-employer PC and that Dropbox is still fed by her with all her personal and professional documents of her present job.

2. She requested an activity log and geolocation to Dropbox and will provide it to this office once received.

Before this office could initiate an inquiry with Respondent, the following clarifications were sought from Complainant by way of an email:

a. Was your ex-employer aware that you were using Dropbox under your personal email address on its personal computer (PC) for business and/or personal purposes?
b. Did your ex-employer have a policy notice regarding resignation? That is, whether you were required to inform your ex-employer about your resignation 1 or 2 or more months prior to your resignation.
    i. If yes, provide the reason why you did not unlink your Dropbox account from that PC during that period.
    ii. If no, again provide the reason why you did not unlink your Dropbox account before leaving the company.
c. Was the PC password protected? To be precise, when starting that PC, were you required to insert a password which was only known by you?
d. What makes you believe that someone else is accessing/using your Dropbox account from that PC?
e. Once you receive the activity log and geolocation from Dropbox, kindly provide this office with same, since images you have provided do not show evidence that someone else is accessing your Dropbox account as this office has noticed you (Complainant) have moved/added/deleted/edited the files.

The Data Protection Office also advised Complainant that whenever she is leaving a company to join another one, to make sure that she removes all her personal details on the personal computer she is using or any other materials to avoid such incidents from reoccurring.

In her reply, Complainant stated that: "

a. Yes, each employee had a personal Dropbox account.
b. I provided 1 month of notice regarding my resignation.
    i. Unfortunately, I removed all my personal files but did not notice that my Dropbox account was still linked to the Computer I was using. At the moment I noticed these manipulations on my Dropbox, I unlinked the account but unfortunately, Dropbox leaves a local folder with those files on the computer physically.

c. ***Yes, the PC was password protected with a password known by the executive directors only. But since I left my employment over there, those executive directors are no more involved in the Company - so I suspect that someone else had got access and hacked my personal Dropbox account with files/content that I have added well after submitting my resignation letter.***
d. ***I got notifications from Dropbox that some files were accessed and modified on a day that I did not connect to Dropbox. Furthermore, I also received confirmation from other employees at Respondent that someone used my computer on that very day and printed out lots of documents - these also included Confidential/Sensitive files from my actual Employee/Company.***
e. ***I'm still in touch with Dropbox over the Log activity and will provide same as soon as I receive it."***

Subsequently, this office wrote a letter to Respondent to request the latter to provide clarifications on the allegations made by Complainant. Respondent was also requested to:

1. permanently delete the Dropbox folder containing the personal information of Complainant from the computer she was using and to uninstall the Dropbox program from that computer. Note: The Dropbox can be installed afterwards and to provide this office with evidence that the folder has been deleted from the computer.
2. identify the person who has accessed, modified and printed out the personal documents from Complainant Dropbox account (Dropbox folder found on that computer) and provide a justification for doing so.

In its reply, Respondent informed this office that:

1. There was/is no Dropbox folder containing the personal information of the Complainant on the company's computer which was entrusted to her. Nevertheless, they have deleted the one Dropbox folder that was on the said computer. (Screenshot was provided as evidence to this office).

2. Despite the Dropbox folder having been unlinked and therefore having no connection with Complainant (or her email address), Respondent has further uninstalled the said program from its computer. Respondent provided evidence as screenshots one before the uninstallation and the other one after the uninstallation of Dropbox.

3. In the course of an internal investigation, Respondent came to know that Complainant was one of its eight former employees employed by a competitor (a company which was set up by one of Respondent former executive directors). The said employees were apparently instructed to save documents relating to Respondent in Dropbox folders created on the devices which Respondent had put at their disposal.

4. Prior to leaving the company all the said employees deleted the Dropbox folders which contained confidential and sensitive belongings to Respondent and further unlinked the said Dropbox folders from the said computers in order to block Respondent's access to

information. Complainant apparently forgot to delete and unlink a Dropbox folder which contained irrefutable proof that the clients of Respondent have been systematically targeted on behalf of the other company (competitor) and that Respondent's resources have been diverted for the benefits of the competitor.

5. The Directors of Respondent have decided to report the matter to the Police and copies of some of the documents retrieved from the computer entrusted to Complainant will be produced to the Police for that purpose.

6. The Board of Directors of Respondent never condoned the alleged practice of employees using Dropbox linked to their personal email addresses to store the Company's information. All employees of Respondent, including Complainant, were assigned an office email (name@companyname.mu) to be used in the performance of their duties.

7. The company denies that any computer belonging to the Company has been hacked. In the course of the internal inquiry referred to above it became known that most of the computers were protected with the same password, namely "1234."

8. No one "accessed, modified and printed out the personal documents" of Complainant.

By means of an email, this office informed Complainant:

1. on the declaration made by Respondent.

2. that according to section 7 (2) of the Data Protection Act 2017, any person who, without reasonable excuse, fails or refuses to comply with a requirement specified in a notice, or who furnishes to the Commissioner any information which he knows to be false or misleading in a material particular, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.

Complainant was also required to submit any concrete evidence to substantiate her allegations in writing to this office following receipt of the email, failure to which the enquiry will be closed. However, Complainant did not respond to the email sent to her.

The Data Protection Commissioner has decided as follows:-

After careful analysis of the evidence of record and given the detailed explanations provided by Respondent, I am of the view that no breach of the Data Protection Act has been detected by this office. Should Complainant have come forward with more concrete proof regarding any unauthorised use of personal data by Respondent, I would have been in a better position to determine whether any potential breach could indeed have taken place. Therefore, the enquiry is closed.