This is a summary of the decision of the Commissioner.

The Data Protection Office received a complaint from Complainant against Respondent. In her declaration, Complainant stated that:

a. After being dismissed, Complainant met the Financial Controller of the company, the latter informed Complainant that he saw the email that she had sent to the region, and that he had been on automatic copy of all her e-mails upon the Country Manager's request and that the Country Manager was also on automatic copy of all my e-mails since Complainant joined the Company.
b. Complainant thus believes that the Country Manager has been reading all her emails, and had access to all her IT accesses without her consent. Besides, she also stated that the Country Manager used the information she had sent privately in her e-mails to pry into her conversations with the Respondent's head office.
c. The Country Manager may have abused his power to pull information from her personal mobile since email provided to her by Respondent was also set up on her personal mobile.
d. Respondent's Management has abused their power and use its IT System to monitor all their employees' moves and private lives.

This office wrote to Respondent to provide clarification on allegations made by Complainant. Respondent replied to this office denying all allegations by Complainant. Furthermore, Respondent stated that the allegation is fabricated, groundless, defamatory, with sole intention to harm the company.

Subsequently, this office scheduled a meeting with the Country Manager now known as Cluster Manager, Financial Controller now known as Country Controller and the IT Administrator of Respondent for enquiry purposes.

Following the meeting with Respondent, this office received the statements of the above person.

a. The Country Controller declared that he did not have a conversation with Complainant concerning emails and neither he nor the Cluster Manager has received email from automatic copy.
b. The Cluster Manager stated that he does not have access "to the email and IT access" of any employee and was not in automatic copy of emails sent by Complainant.
c. The IT administrator declared that the company does not have an automatic copy of theemail system since Respondent has a very strict infrastructure. The email accounts of employees are created in Philippines.
d. Respondent also provided the following documents:
    i. Respondent's End User Security
    ii. The Email/Internet Guide
    iii. Acknowledgement Note signed by Complainant acknowledging that she has received copies and read and understand the following documents: Code of Business Conduct, Respondent Corporate Business Principles, Respondent Human Resources Policy, Respondent Management & Leadership Principles,

Executive Guide to Information Security, Email/Internet Guide and Respondent End User Security Policy.

Consequently, this office scheduled a meeting with Complainant for enquiry purposes. On the same day, Complainant forwarded this office the email she had sent to Respondent's Regional regarding her termination with immediate effect.

Following the meeting with Complainant, the latter requested the Data Protection Office to investigate the matter and look into it from the email recipients' laptops to shed light on how they had access to any email that was sent from Complainant's email address.

This office has also sent an email to Respondent Regional (Kenya) requesting the latter to confirm by verifying Respondent server whether :

a. there was an automatic copy on Complainant 's email to the Cluster Manager and the Financial Controller.
b. a copy of the email with subject "Termination with immediate effect" dated 14 October 2016 was received on Cluster Manager email and who was the sender.

This office further wrote to the Cluster Manager to clarify on the monitoring of emails by Respondent.

The law Chambers representing Respondent replied in response to the above email addressed to the Region and the letter addressed to the Cluster Manager to inform this office that:

a. The Company confirmed with experts in Nairobi, Switzerland and IT Security in Australia that at no point the emails of Complainant were automatically copied to the Cluster Manager or to any other employee.

b. Moreover, the email in question "Termination with immediate effect", on 14 October 2016 was sent to the Mauritius HR Executive who in turn forwarded the email to the Cluster Manager and the Cluster Controller for their attention.

c. The Company reiterates that it does not monitor the email accounts of its employees but however has the right through its technicians to monitor the use of the email system in accordance with applicable law when there is evidence of serious misuse.

A site visit was conducted by the Data Protection Office on the premises of Respondent and the following observations were made:

1. Complainant sent an email with the subject "Termination with immediate effect" on 14th October 2016 at 10:16 a.m. to Respondent Regional Office and the latter copied the email to Respondent legal services, Respondent Human Resources and the Mauritius HR Executive. The Mauritius HR Executive, in turn, forwarded this email to Cluster Manager and Country Controller on 14 October 2016 at 10:19 a.m. A copy of the email received by the Cluster Manager and Country Controller was provided to the Data Protection Office.

2. A second email with the subject "Fwd: Termination with immediate effect" was sent by Complainant on 14th October 2016 at 11:04 a.m. to Respondent Regional Office and Complainant

copied the email to Respondent's legal services, Respondent's Human Resources and the Mauritius HR Executive. The Mauritius HR Executive, in turn, forwarded this email to the Cluster Manager and Country Controller on 14 Oct 2016 at 11:05 a.m. A copy of the said email was provided to the Data Protection Office.

3. The laptop which Complainant was using is locked and this office was informed that all accounts at Respondent are deactivated if not used after 1 month.

This office then informed Complainant on the enquiry conducted and that so far there has been no evidence against the allegations made. The complainant was thus required to submit any concrete evidence to substantiate the allegations made within 21 days, failure to which the enquiry will be closed.

The Data Protection Office also contacted the Barrister at law representing Respondent on whether Respondent had any further views or update with regard to this complaint. Respondent's Barrister at law replied as follows: "I can confirm that the client, Respondent has confirmed that:
'no further issue arose post the complaint at DPO, except for a Plaint with Summons (PWS) received on 04 Aug 2017 ...'"

By way of an email, this office contacted Complainant to inform the latter to submit any update if any and that since the breach of contract case is before the Supreme Court, the enquiry is being closed.

Complainant replied stating that the Breach of Contract Case had indeed been lodged in the Supreme Court. Complainant also informed this office that following her complaints the person responsible at Respondent has been suspended from his function in August 2017 and permanently terminated since December 2017 following an internal investigation by Respondent including the set up of a disciplinary committee to evaluate his actions.

Thus, this office contacted the Barrister at law representing Respondent to provide clarifications on the statement provided by Complainant. Respondent's Barrister at law replied to this stating that: "I am informed by my client that the previous CEO employment was terminated for reasons unrelated to the subject matter of the complaint being investigated by you."

The Data Protection Commissioner has decided as follows:-

The data protection issue before me is whether there has been an alleged monitoring and/or automatic copying of the emails sent by Complainant to Respondent Head Office without the consent of the former.

A site visit was undertaken by this office at the premises of Respondent to investigate on how the Cluster Manager and the Country Controller became aware of the email sent by Complainant to Respondent regional on 14th October 2016. The laptops of both the Cluster Manager and the Country Controller were verified and it was observed that the Mauritius HR Executive (who was in copy of the said email) received Complainant's email on Friday 14th October 2016 at 10:16 a.m. and then the Mauritius HR Executive

forwarded the said email to the Cluster Manager and Country Controller on the same day at 10:19 a.m. Evidence regarding the forwarding of the email was submitted during the site visit.

The findings of the enquiry have also revealed that Respondent has appropriate organisational measures in place such as Respondent End User Security Policy and the Email/Internet Guide. Moreover, staff is required to sign an acknowledgement note that they have read and understood these policies.

After careful perusal of the investigation carried out, I am of the view that no evidence of any such breach has been detected in order to reach the conclusion that an offence under the Data Protection Act has been committed. Respondent has also satisfied this office that it has appropriate security and organisational measures to protect the processing of personal information within the company. However, Complainant's termination of employment based on her performance is a suitable case under the Employment Rights Act and not within the jurisdiction of this office.