REF.NO:-DPO/DEC/9

IN THE MATTER OF:-

Complainant

VERSUS

Respondent

A complaint was lodged on 22 September 2011 at the Data Protection Office under section 11 of the Data Protection Act against Respondent based on the allegation made by the latter against Complainant for having written an anonymous complaint letter dated 14 February 2011 to the Data Protection Commissioner with regard to unsolicited emails sent on her office email address. Complainant alleges that further to the anonymous complaint which she never made, she was suspended with immediate effect from her post of Senior Administrative Assistant by Respondent on grounds of misconduct by way of letter dated 5 September 2011 from the Human Resource and Administration Manager of (…) and subsequently upon her request, on humanitarian grounds as averred by Respondent, an agreement of early retirement was concluded on 24 November 2011 and disciplinary action was stopped. Respondent in its letter dated 5 March 2012 addressed to this office clearly stated that *"ultimately … (Complainant) has not been sanctioned in any manner for having sent a letter to the Data Protection Commissioner as all charges have been dropped against her following the agreement."* A copy of the agreement signed between Complainant and Respondent has also been filed at this office.

This office has indeed received an anonymous complaint namely *Anonymous versus* (…)where the latter (an employee of (…)) in that case had allegedly emailed symbolic pictures of a religious nature to several persons using their email addresses without their authorisation. In so doing, he has allegedly divulged the private email addresses allocated to employees of (…) including Complainant to unauthorised individuals copied in the same email. Respondent in that case, (…), massmailed to different individuals on 7 February 2011 at 10:42 am and one among themwere(…), Complainant in this case.

By way of letters dated 5 September and 16 December 2011 addressed to Complainant, 3 charges were preferred against Complainant, one of them being that the latter has addressed without authorisation or consent of Respondent, her employer, an anonymous letter to the Data Protection Commissioner from her email box allocated to her by Respondent and which has caused serious prejudice to it and which is of relevance for the purpose of this enquiry.

Furthermore, Respondent in its letter dated 5 March 2012 stated that soft copies of the prejudicial anonymous letter were recovered from the PC assigned to Complainant which was also annexed in the same letter, following an audit trail carried out at random on four computers within the premises of (…). Complainant has further alleged that the (…)password given to her was not confidential and there was no option to change the default password. It is the support department of (…)which has given her the login name and the password "(…)". She does not have the change option for password at expiry. She used the same password set up by IT department which is (…). There have been three interventions on her PC regarding password problem in December 2010, March 2011, and August 2011. There has never been the signing of an e-mail policy regardinge-mail allocation to her by Respondent. Complainant has also added thatRespondent has not given her responsibility of the PC which she was using.

The enquiring officers have enquired with (…) whether they were aware that the password given to Complainant was (…) and whether there was an option to change the password by the user. Respondent was further questioned about any option for password change as it is a good practice for any organisation to provide a system whereby users can change his/her password at the first log-in. Respondent replied by way of letter dated 30 May 2012 addressed to this office as follows:

"(…) Eligible officers of (…) are provided with a PC to conduct their daily business activities and the use of computers is subject to strict procedures which are imparted to the users. Each user is initially provided with a unique username. On first login to their PC, each staff is required to change their password and this is enforced by the policies set on the server. It should be noted that passwords for all users expire after 30 days and users are required to change their passwords. Failure to change the password will result in the account being automatically locked.

Our record from the (…)Helpdesk shows that (…)made a request in August 2011 concerning a password problem on her pc. The request ID assigned is (…) and request details are "System could not log me on". Further to the intervention of a (…) engineer, it was noted that (…)had forgotten her password and could not log on to her PC. The password was reset by the IT engineer and changed by (…)to be able to log on her PC."

Respondent also replied that Complainant *"was responsible for changing and safeguarding her own password. Details of the problem resolution for ID (…)are: "User forgot password. Password has been reset and changed by user.*

(…) all users must mandatorily change their passwords every 30 days which is enforced at the server level. Moreover a user has the option of changing his/her password at any point in time.

(…) All assets provided by* (…) *to the users, including computers, are the sole property of* (…). *However, the security, usage and care of these assets fall under the direct responsibility of the respective user, who is also responsible for its proper use and content. The complainant had full responsibility of her PC as an employee of* (…).*"

(…) was further questioned whether the password given to the complainant was confidential. Respondent replied that "(…) ***on request from* (…)*the password was reset and* (…)*was required to use her own password upon login. She was therefore entirely responsible for supplying and safeguarding of her password, although it must be stressed that the password is not for her personal use but rather for her professional activities."***

(…)was also required to show to this office how the contents found on the PC of Complainant fall within the responsibility of the user. Respondent replied that "(…) ***the contents found on* (…)*PC fell under the direct responsibility of the latter, the more so that the contents were stored in the user profile of* (…), *which only* (…)*has access to and the attributes of those contents show that owner and author was* (…).*"***

The enquiring officers asked Respondent whether there is a written contract between the employees and (…) that all materials found in the PC of the employee using it, is within his/her responsibility. Respondent replied that "(…) ***there is no express written provision to stipulate that a user has the responsibility of the content found on the PC attributed to him/her but it is a usual and normal business practice at* (…) *that such is the case and this is known and accepted by* (…)*employees. Moreover, the code of conduct in force at* (…)*and which is binding on employees does recommend employees not to make any unauthorised or lawful use of* (…)*resources."***

Complainant also added that according to (…), when the former phoned him on 5/9/2011 and enquired about her PC, the latter said that Messrs(…)had taken her PC on 3/9/2011 for investigation.

The enquiring officers asked Respondent whether official permission was granted for the officers of (…) to carry out any investigation on Complainant's PC on 3/9/2011. Respondent replied, "(…) ***following anonymous letters which were sent to various local and foreign authorities and copies of which were remitted to* (…) *by Police through the Ministry of ICT, an internal enquiry was opened at* (…). *An audit trail was carried out at random on four computers.***

Respondent also replied that"*an authorisation was granted by the General Manager of* (…) *to the IT team to perform an audit trail."***

Complainant allegedly reported this matter to the HR department that she was not there (since 3/9/2011 was a Saturday) and without her permission and presence, they have taken her PC and she informed them that if anything happened on her PC, it would be their responsibility.

The enquiring officers have asked Respondent whether the investigation of 3/9/2011 was carried out by an IT team from (…) and whether there is an implicit or explicit procedure allowing(…)to take any PC from a staff for investigation purposes. Respondent replied that *"(…) all PCs found at* (…)*are the exclusive property of* (…) *and there was absolutely no need to give advance notice of the audit to users or officers of* (…) *as the purpose of an audit would have been defeated.* (…) *did not need the presence or permission of any officer, and more specifically that of* (…)*to carry out the said audit exercise. (…) In fact, the PCs of several users were handed over to the IT team to conduct the audit and there has not been the least protest or complaint over that audit exercise."*

Complainant also added that regarding the e-mail sent by(…), out of the 20 persons who received the mail, 8 employees are housed on the same floor as the complainant, i.e, on the third floor.

This issue was also raised with Respondent who replied that *"(…) the* (…) *IT team does not have the password of any user at* (…)*. Each user is required to insert his/her personal password at first login and after each subsequent password expiry period. The respondent maintains that no other person working at* (…)*, whether on the third floor or elsewhere, had any access to or worked on the PC attributed to* (…)*for her official work."*

Complainant has also pointed out that the officer who has certified that the letter in lite was on her PC, did not do so in her presence. Complainant alleged that they all know the password (…). Respondent was also asked to provide clarification on this issue whether they think that it was appropriate to carry out such an investigation in the absence of Complainant.

Respondent replied:

"*(…)*did not and could not know before carrying out the audit exercise whether anything incriminating would come out of any of the four computers. Had the result been negative, the exercise would have continued on other computers until* (…) *would have been satisfied that no computer at* (…)*had been used to write anonymous letters whose content was incriminating and false. Therefore the issue of doing the audit exercise in the presence of* (…)*did not arise for the above mentioned reasons."

Furthermore, Complainant has stated that she has not seen where this letter has been saved on her PC, on which folder and at what time nor has she seen a print screen of it.

Complainant added that (…)has acted as a guarantor of anEWF loan for her on 2 August 2011 and she cannot understand why this charge has been put against her as she would never want to put him into trouble. Respondent was asked whether Complainant has any conflict at work with (…). Respondent replied that *"(…)was not aware that (…)had guaranteed a personal loan for the complainant as this is a personal matter between two individuals, therefore the issue of conflict arising in having (…)and (…)working together never cropped up."*

Complainant has also added that her place of work is on the third floor and she has to move to her Manager and other colleagues of the same department who are on fourth and sixth floors approximately 8 times per day by leaving her pc on and open. This issue was also raised with Respondent whether there was an automatic windows lock setup in the PC of Complainant and whether there was a minimum time for the PC to be locked which would require user authentication to log in again. Respondent replied: *"(…) all PCs are automatically locked in (…)whenever there is no user activity for fifteen minutes. When a PC is locked, the respective user is required to log in by supplying his/her password. (…)had the sole responsibility of locking or securing the data of the computer under her control while she was moving around."*

On 14th February 2011, from 13.30 to 16.30 p.m, Complainant was allegedly upstairs on the sixth floor preparing and attending a Procurement Committee. Her PC was open and according to her anyone can log in since there was no confidential password. When she moved from the third floor to the fifth floor, in August 2011, it was (…)himself who arranged for moving and setting up of the pc and (…)had changed the keyboard of her pc on 1/9/2011. Respondent reiterates that *"the password for each user is confidential and its usage falls under the direct responsibility of the user."*(…) also added that *"Should her allegations that (…) might have inferred with her computer be true, which are hereby expressly denied, for the sake of argument, she would still have herself to be blamed."*

(…) concluded that *"(…) it is significant to note that one of the charges against (…)was to the effect that she had sent an anonymous letter to your office without the authorisation of (…). The subsequent voluntary agreement reached between (…) and (…) following disciplinary proceedings initiated against her has therefore put an end to all disputes arising between herself and (…) having regard to her employment with (…), including the present matter.*

Secondly, (…) has not used, misused or has otherwise dealt with any of the personal data of (…). The mail address, login and password are assigned to her, although loosely called her personal mail and password respectively do not form part of her personal data in as much as such mail address and password are assigned to her by virtue of her employment and form part of the intellectual property of (…). Since her retirement, the mail address, login and password assigned to her have been de-activated."

Complainant was further contacted to attend to a meeting at this office on Wednesday 13th June at 14.45 to reply to the averments of Respondent. Complainant did not come but sent an email whereby she insisted that she has not sent the anonymous letter though it was found on her PC. The enquiring officers advised Complainant to be more responsible as regards security issues related to a PC for the protection of her own personal information as credentials like username and passwords are meant to be strictly confidential.

A site visit was carried out on 15.06.2012 at (…) to verify the contents of Complainant's PC. (…)accompanied the enquiring officer to verify the content of the PC allocated to Complainant.(…) and his team were informed to secure the PC of Complainant which was done as well as being kept in a locked room.

Finally, the enquiring officers contacted Respondent by mail on 19 June 2012 to know how the anonymous letter allegedly sent by Complainant has been prejudicial to (…)as averred. Respondent through one (…)replied that *"(…) the letter is prejudicial to* (…)*because an internal communication between two employees, using the internal network of* (…) *which is meant for professional activities only, has triggered an enquiry from a public body without the knowledge of* (…)*. One of the employees has even received a warning from your office. The other officer is now causing trouble and annoyance to* (…)*by making false allegations against* (…)*, which is itself the subject of an enquiry whilst it has been kept in the dark all along.* (…) *is in fact a victim which is being turned into a suspect. I hope that* (…) *has replied to your query satisfactorily and that these harsh facts do amount to prejudice in the eyes of the Data Protection Office."*

The Data Protection Commissioner has decided as follows:-

Firstly, there is no legal requirement in the Data Protection Act which obligates all complainants wishing to lodge a complaint with this office to mandatorily inform and obtain permission of management before lodging a complaint with this office and which is not even directed against the employer. As regards the initial anonymous complaint lodged with this office against (…), an employee of (…), all decisions of the Commissioner are posted on its website, without the names of the complainant and the parties involved being quoted to protect the confidentiality of the personal information of the persons involved as per the requirements set out in section 6(3) of the Data Protection Act by which this office is bound. Therefore, (…) cannot in any circumstance claim of having been kept by this office "in the dark". Under section 11(b), all decisions of the Commissioner are made known to the complainant and copied to the respondent involved in the case, by way of letter. Since, (…) was not the complainant nor the respondent in the mentioned case, it was not made aware of the decision of the Commissioner, by way of letter. The Commissioner would like to appreciate that an institution of the calibre of

(…) is indeed aware of the legal parameters set out in the Data Protection Act as regards the procedures laid down for the conduct of enquiries.There is thus no dispute on the fact that once a complaint is lodged at this office, all parties to the case would be informed of the outcome of the enquiry.

The opinion of the Commissioner is clearly reflected in section 38 (1) (e)&(f) of the Employment Rights Act which provides:-

"An agreement shall not be terminated by an employer by reason of –

(e) the worker's filing in good faith of a complaint, or participating in proceedings against an employer involving alleged breach of any terms and conditions of employment;

(f) a worker's exercise of any of the rights provided for in this Act or other enactment, or (…)."

It would seem that if the reasoning of Respondent is applied, all complainants wishing to seize this office for action, have to be, a priori, authorised by management to exercise their rights. Should the management of Respondent not be agreeable, then the person should not lodge a complaint. The Commissioner would like to point out that this particular course of action would be tantamount to a clear breach of the principles enunciated in our constitution, the Data Protection Act and the Employment Rights Act.

In this context, the Commissioner is also of the view that complainants have rights embodied under the Data Protection Act which allow them as data subjects whose rights have been violated, to appeal to the Commissioner to recommend corrective measures and/or prosecute those at fault. If a complainant, employee of a particular institution, feels that his privacy rights have been violated during his employment, he may lodge a complaint at this office without fear of being reprimanded or subject to a warning or dismissed because a complaint has been lodged at this office. The right to lodge a complaint cannot be defeated by the fact that the employee has not informed management of the nature of the complaint which is not even directed against the employer and the latter cannot under any circumstance, use a complaint made to this office as a weapon for potential dismissal and for the conduct of disciplinary proceedings on theground that Complainant has lodged a complaint which is indirectly prejudicial to it being given that the latter has allegedly made a complaint against another colleague who has sent unsolicited emails to other colleagues or people. This is indeed a violation of the sacrosanctity of the right to legal action.

Secondly, true it is that the complainant had the operational responsibility of the PC allocated to her for the performance of the functions entrusted to her. However, it has not been proven beyond reasonable doubt by respondent that the complainant is in fact the person who sent the anonymous letter to this office. It is indeed not sufficient and/or irrebutably automatic that a person commits an unlawful act simply by the mere fact that the anonymous complaint letter in lite is to be found on a PC which was being used by her during office hours. This is a rebuttable presumption if a presumption of fact is assumed to exist here. The gist of the complaint made to this office relate to the fact that an anonymous letter was sent to this office regarding numerous unsolicited email communications being sent to various parties by an employee of (…) (not a party to this present case) of a religious nature, which was also by coincidence sent to the complainant, and this is claimed to be allegedly prejudicial to (…). This office entertains no jurisdiction to enquire into the reasons which have prompted Complainant to sign a voluntary agreement between herself and Respondent with regard to the suspension and early retirement of Complainant. However, this office does have jurisdiction to enquire upon whether there has been a violation of the data protection rights of complainant with regard to her personal information having been misused by a third party to her detriment namely by a potential unauthorised use of her password which led her for being taxed of sending an anonymous letter to this office of prejudicial nature to Respondent. It is important to highlight here that a password, in principle, belongs to the user and is thus personal information not meant to be shared with others.

Although the charges attached to the disciplinary proceedings against Complainant were dropped-one of the charges being:-*"You have, without the authorisation or consent of your employer,* (…)*, addressed a letter to the Data Protection Commissioner with regard to the receipt of messages in the email box allocated to you by* (…) *and which belongs to* (…)*, which letter has caused serious prejudice to* (…)*."*- the point remains that Complainant had to enter into a voluntary agreement of early retirement based on the charges preferred against her. Had there been no charges, logically, Complainant would not have been required to enter into the mentioned agreement.

Although Complainant has denied being the author of the anonymous complaint against one of her colleagues and which Respondent has not been able to satisfy this office that Complainant is indeed the author, it is quite clear that Complainant cannot be held totally responsible for a PC belonging to Respondent found in a quasi-public office place.In fact, investigation has revealed that an administrator acting as an ethical hacker can access any windows system provided that permission is granted for investigation from management, which is the case here. Therefore, although Complainant was working on the PC allocated to her, she cannot be held liable for theunauthorised use of a password also known to the IT department.

Respondent is therefore informed that although this office does not have the legal powers to probe into the circumstances of the retirement of complainant, it would urge Respondent to adopt the required measures to protect the personal information of its employees by ensuring that adequate organisational and technical safeguards are taken to avoid the recurrence of such incidents whereby other parties may have unauthorised access to PCs not allocated to them.

Under section 27 of the Data Protection Act, a data controller is required to take appropriate security and organisational measures for the prevention of unauthorised access to the personal data in his control and ensure that the measures provide a level of security appropriate to the harm that might result from the unauthorised access and the nature of the data concerned. A data controller is further required under this section to take all reasonable steps to ensure that its employees are aware of and comply with the relevant security measures.

Failure to abide by the provisions of this section may result into prosecution by this office.

MrsDrudeishaMadhub

Data Protection Commissioner

Data Protection Office

Prime Minister's Office

4th floor, Emmanuel Anquetil Building,

Port Louis

12.07.12