**REF.NO:-DPO/DEC/10**

**IN THE MATTER OF:-**

**Complainant**

**VERSUS**

**Respondent**

**A complaint was lodged on 03.10.11 at the Data Protection Office under section 11 of the Data Protection Act against Respondent which pertains to the alleged unauthorised forwarding of personal data by the latter as an employee to her personal email address.**

**Complainant by way of written declaration to this office dated 3 October 2011, averred that Respondent had joined the company as accounts officer on 12 January 2009 and submitted a letter of resignation to the company on 06 September 2011which is further subject to a notice of 3 months as per her contract of employment and her last day in the company would have been 05 December 2011. However, her contract of employment was terminated before the expiry of the term of 3 months by Complainant, her employer.Moreover, Complainant averred that following discussions with the Human Resource Section, the company had already decided to remove the present responsibility from Respondent, even before her resignation.**

**On 30.09.11, Respondent has forwarded from her office email address to her personal email address, confidential files of the company namely 6 'chrono' excel containing payroll details for the month of August 2011.**

**Complainant by way of a second declaration recorded on 5 October 2011 further informed this office that Respondent had allegedly sent 3 unauthorised emails from her office email address:-**

**The first email dated 30 September 2011 was sent to both Respondent's office email address and copied to her personal email address. The email contained attachment documents, namely 6 'chrono' excel, containing payroll details for the month of August 2011 with employees' names, salary, details of the calculated salary amount (NPF, PAYE), car allowances, overtimes, loans and transport.**

**The second email dated 28 September 2011 was sent to Respondent's office email address and contained names of suppliers (company names) and invoice details.**

**The third email dated 03 October 2011 was sent to Respondent's office email address and contained the logistics for staff leaves planner with the names of employees and leaves' details.**

**Screenshots of the above 3 mails have been submitted by Complainant to this office. Complainant stated that the content of the emails forwarded were verified by both the IT Manager and herself. Complainant also declared that the office email address is accessible outside office.Complainant mentioned that there are security measures in place in the company to secure information namely an active directory of all employees where management defines access of employees. Furthermore, audit is carried out on the server to monitor access of employees on files. Respondent, however, stated that based on the company's nature of business, no outgoing email can be controlled and that there are no preventive measures taken when employees resign and their access remains the same.**

**Complainant also added in her statement that in the event that a staff resigns, the latter's outgoing emails are monitored by the IT manager to avoid any leakage of information. Furthermore, all employees who join the company are required to sign a contract incorporating data protection principles as well as a confidentiality chart. As per Complainant, Respondent had previously made a request to take an office file to complete at her residence, and the request had been authorised by the Director herself. As stated in Complainant's letter dated 22.05.12, she confirms having given permission once to Respondentto complete a task at home after verification that no confidential document was involved although there is no written evidence of such permission given to the latter by Complainant.**

**Respondent by way of declaration dated 30.11.11, informed this office that she was appointed as accounts officer at (…) in 2009. Her main duties were to work in the finance department and to perform accounts payable, accounts receivable, bank transaction, payroll, statutory returns for VAT, PAYE, NPS, APS and other administrative or finance issues.**

**Respondent also stated in her declaration that upon joining (…), the company provided her access to the server containing information of the company, the internet and email facility (both internal and external mail). External mail was granted to all staff and could be accessed outside the company. Moreover, Respondent informed this office that external mailing facility was required as part of her job role in order to liaise with clients, banks and suppliers.**

**Respondent acknowledged having sent the email dated 30 September 2011 with the payroll details of August 2011 to her personal email address (…). She also averred that 30 September 2011 was the last day to submit NPF return, and being given that the (…)website to upload the return was very slow, Respondent was unable to send the return in the office. Consequently, she forwarded the payroll sheet on 30 September 2011 by email in order to work out the NPF at home as she was not authorised by the finance manager to stay after 17:30p.m in the office.**

**Respondent also pointed out in her declaration that if the return was not submitted on the deadline date, (…) would have received penalties. An audit trail report from (…) was submitted to this office by Respondent as evidence that she worked at home. Respondent stated that she had logged in the (…) website using her user id at 19:55p.m on 30 September 2011. Respondent also stated that she had checked each employee, edited their NPF return and verified with the alleged payroll of August 2011 on whether the amount of NPF tally with the return submitted. Respondent also informed this office that the return was completed at 22:21p.m on 30 September 2011.**

**Respondent admitted and had tried to justify why she had to do so to her directors, but the finance manager said that the return was supposed to be submitted on 30 September at 15 pm and not 22 pm. Respondent stated that she was suspended with immediate effect.**

**As per Respondent's declaration, she did send the email on payroll details to her personal email address but was not sure whether on 30 September 2011, she had sent theemail on payroll to her office email address since on 6 October 2011, (…), also director at (…), asked Respondent to login on her personal email address on his laptop. (…)forwarded the alleged email to his email address (…) and deleted the email from Respondent's personal email address. Respondent stated that she had sent the alleged mail to her personal email because very often when she connected on the webmail**

**outside office, the system was unavailable. Respondent did not want to take any risk on the deadline date.**

**Respondent also acknowledged forwarding the email on local/sick leave to her office email address. Respondent averred that she did so in order to update the file on employees' leaves for September 2011. Respondent added that she was receiving daily emails through the receptionist to update the local and sick leave sheet and she had been informed by the finance manager to update the sheet up to September 2011 for handing over to the Human Resource Assistant. Respondent advised that since she was taken up with accounting tasks during the day, she forwarded the alleged email in order to complete her job only.**

**Respondent also stated that regarding the mail on accounts payable, the file contained only corporate data and that she had forwarded the file on her office email address to check which suppliers to process payment and issue cheques on the following day.**

**Furthermore, prior to September 2011, she had not asked for authorisation to take documents home by email because before, she used to reach office early morning, leave office late and was authorised to work on saturdays to complete her work. However, she had been asked not to come before 8 am and not to stay after 17:30 pm in the office. Also, Respondent stated in her declaration that she did not ask for any authorisation to send the emails as she was aware that all incoming and outgoing mails were monitored by the director.**

**Respondent also informed this office that she had signed a confidentiality chart with (…) in August 2010 but she had not been able to go through the document well as she did not get a copy. Respondent also stated that she has a vague knowledge about Data Protection.**

**Finally, Respondent told that she sent the emails with the intention of completing her daily office tasks only. She also mentioned that the director(…)told her that he preferred that she leaves office immediately and that he would not go to the Data Protection Office or the Cybercrime Unit. Respondent further averred that she has acted without any bad intention and was only doing her work.**

**Further investigation was carried out by the enquiring officer regarding the exact date and time that the payroll and NPF process was completed for the month of August and September 2011.**

**Regarding the above, Complainant provided this office with the dates that salaries and NPF amounts have been debited from their accounts, together with a copy of bank statements and NPF returns for August and September 2011. As per Complainant's letter dated 22.05.12, NPF amount for the month of August 2011 was debited on their account on 03-Oct-2011.**

**Following further enquiry, Complainant highlighted in her declaration dated 29.05.12, that the (…) upload for the month of August 2011 was done on 28 September 2011 starting at 18:15 and completed at 18:24 p.m. Complainant provided the office with a copy of audit trail report from (…).**

**This office conducted an enquiry with (…)on 01 June 2012 to confirm the exact date and time that the upload for NPF August 2011 was completed by (…). As per reply from (…), the NPF return on (…)as sent on 30 September 2011 at 22:21 p.m. (…)also sent a copy of the log detailing the actions on that return.**

**It has been noted that in the NPF return document submitted by Complainant for September 2011, the return had been performed on the ID (…) under the name of (…). However, as per Respondent's declaration dated 18.06.12, the last NPF return done by her was for the month of August 2011 and not September 2011. The enquiring officer further queried Complainant on this discrepancy. Complainant then stated that the NPF for September 2011 has been performed by (…)using the ID number (…)until a new ID be created under the name of (…). It is noted as per Complainant's declaration that a request to create a new ID has been made by (…)to (…) on 16.12.11 and a new ID was provided on 18.12.11.**

**As per Complainant's letter dated 22.05.12, the policy of (…) on confidentiality is contained in the employee's manual. An extract of the relevant part has been submitted by Complainant. Complainant also added in her declaration dated 29.05.12 that the 'charte de confidentialite' has remained same and unchanged since 2009. Complainant also stated that a copy of the 'charte de confidentialite' is given to all employees on receipt. Complainant has provided this office with evidence that a copy was given to**

**Respondent by way of letter dated 04 July 2012, enclosing a copy of the employment contract and employee's manual signed by Respondent. Moreover, for the 'charte de confidentialite', Complainant mentioned that no proof that same has been given to Respondent can be retrieved in the files.**

**As per Respondent's declaration dated 18.06.12, Respondent has signed the employee manual to which is annexed the 'charte de confidentialite'. However she was not provided with a copy and also does not remember if she had signed any document acknowledging receipt of the employee manual and 'charte de confidentialite'.**

**As per Complainant's declaration dated 29.05.12, the personal email of Respondent is inaccessible to a third party. Furthermore, it is also impossible for (…) to verify the personal emails of employees without their authorisation.**

**Respondent confirmed in her declaration dated 18.06.12 that on the 06.10.11, (…)asked Respondent to log in her yahoo mail at (…) office, asked her to put her user name and password, verified if the mail was still in Respondent's inbox and forwarded the mail to his email address (…). He then deleted the mail in sent items, inbox and trash. Respondent also added that she does not have any evidence to prove her say.**

**As per Complainant's declaration dated 05.10.11, the email that was sent on 28 September 2011 contained the names of suppliers which are only companies. Respondent also confirmed in her statement dated 30.11.11 that the suppliers are only companies. However, following further enquiry with Complainant, it was confirmed by way of letter dated 22 May 2012 that the list of suppliers also contained individual suppliers. Respondent also confirmed that although she stated previously that the accounts payable document contained only company names, it may happen that a supplier is an individual like a sole trader doing business by his name. In that circumstance, his individual name would be found in the report.**

**Following further enquiry with Complainant, the latter declared that the email dated 30 September 2011 also contained a sheet with the personal details of employees for previous fiscal years (2009, 2010, 2011).**

**Respondent confirmed in her declaration dated 18.06.12 that the sheet NPF 2009-2010-2011 – 29 July 2011 is used as a control sheet in order to check calculation for payroll.**

**She emailed herself this document in order to cross check figures for August 2011 before sending the return to (…).**

**Complainant also confirmed in her declaration dated 29.05.12 that it is impossible to verify previous logs to confirm whether Respondent used to send company information previously by email. Also, Complainant stated that the company has a webmail which enables staff to access their email even outside office. However, the webmail system facility is given to all staff and does not enable the company to select it for certain staff only. Complainant in her letter dated 22.05.12 addressed to this office stated that forwarding personal details of individuals, is an act of leakage of information that may be detrimental to the company.**

**Respondent confirmed in her declaration dated 18.06.12 that she did not disclose the information to any other unauthorised party. Furthermore, Respondent added that she does not have any physical copy of the document and neither any copy in her email, usb, laptop or any storage media. Respondent also added that her personal laptop has been checked by the(…) IT manager. Respondent stated again that she has sent the information to her personal email only for work purposes.**

**The Data Protection Commissioner has decided as follows:-**

**True it is thatan employee should seek the authorisation of her employer before transferring confidential information from her office email address to her personal email address, albeit for work purposes in accordance with Article VII of the chart of confidentiality and the non-respect of the Chart has led to the termination of the appointment of Respondent under Article XV of the Chart.**

**However, the contractual agreement which Respondent has signed clearly stipulates in its section on *'obligations of the employee'* that the employee bears the duty not to use or divulge or communicate to any person any confidential information which could reveal to be detrimental to the employer. Respondent has further signed an acknowledgement of having received a copy of the employee manual to which is annexed the chart of confidentiality whereby she confirms having read and understood the contents of the documents mentioned.It is important to highlight here that theoffice email address is also accessible outside office andthat the content of the emails forwarded were verified by both the IT Manager and Complainant. No improper use of the confidential**

**information forwarded had been detected by the employer.The employee manual further provides in its section 3.2 '*Non-Disclosure/Confidentiality*' that '*employees who improperly use or disclose trade secrets or confidential business information will be subject to disciplinary action'.***

**Since Respondent has not used the information transferred for illegal purposes but only for work purposes and in the benefit of the employer in accordance with the section on '*required confidentiality*' in the contractual agreement and has already resigned from the company, the Commissioner is of the view that no offence has been committed and/or proven beyond reasonable doubt under the Data Protection Act to warrant prosecution being given the fact that no *mala fide* or criminal intent has been detected from Respondent during our enquiry.**

**MrsDrudeishaMadhub**

**Data Protection Commissioner**

**Data Protection Office**

**Prime Minister's Office**

**4th floor, Emmanuel Anquetil Building,**

**Port Louis**

**19.07.12**