Ref: DPO/COMP/18

I received complaints from two officers of an organisation for unauthorised disclosure of personal data. Respondent 1 was the chairman and Respondent 2 was a member of the Board of Directors of the organisation. Respondent 2 was also the representative of Employees of the organisation. It was alleged that the personal data namely the National Identity Card Number, address and salary details, amongst others of Complainant No. 1 were disclosed without her consent, express or otherwise, and without any legitimate, lawful objective or excuse as they were published in an Internal Audit Report compiled by the complainant's organisation. Extracts of the internal audit report comprising of Complainant No. 1's data were also published in the written press.

The extracts were reproduced in a pamphlet allegedly distributed by members of Employees' association. References were made therein to "une …… Supervisor" and Complainant No. 1 avers being the only woman working as the concerned Supervisor in the department. Parts of the pamphlet, and some materials relate to Complainant no. 1 as averred by her. The latter further stated that disclosure of the data has caused her great prejudice and distress.

The Complainant declared that:-

"It was brought to our attention that the Internal Audit Report had collected, used and disclosed comprehensive personal and sensitive personal data of a few members of Workers Union, including their salary details. On 2 December 2011, we caused a Notice Mise en Demeure to be served on the Managing Director as well as the Chairman and Members of the Board of Directors warning them of the possible contraventions of the Act. We further recommended in the said Notice Mise en Demeure that the Board of Directors and Management take all the necessary and consequent measures to ensure that the personal data of our members be secured and not unlawfully disclosed. However, the organisation failed in its duties to provide appropriate security and organisational measures in as much as:

The Workers Union has officially asked for a copy of the Report from the organisation but this request has been declined on the basis that the report is confidential.

The complainants have also attached documents of mail correspondences between the Workers Union and the management of the organisation, extracts of the internal audit report, newspaper

extracts of allegations of leakage of internal audit report at the organisation and an electoral pamphlet by employees association, as documentary evidences to the complaints."

My office opened an inquiry and the complainants were asked to throw light on the above matter. The respondents were required to provide explanation for the disclosure.

A reminder was also sent on 05 July 2013 to the Legal advisor representing Respondent 1 but no response has been received after several other attempts. Complainants were also requested by letters dated 7 November 2013 for further particulars as to who brought to their attention that the internal audit report was unlawfully disclosed but no response was received. These further queries have thus delayed this case more than it was expected.

However, being given that this office has to conclude its enquiry in presence of the existing evidence gathered to avoid justice being denied, the Data Protection Commissioner has decided as follows:-

Disclosure of structured sensitive personal information concerning a living individual by the data controller is 'processing' within the meaning of section 2 of the Data Protection Act (DPA), irrespective of whether the disclosure is to a member of staff, to a third party outside the data controller's organisation or to the data subject himself or herself. The information disclosed is not of a public nature as provided by law and therefore not exempted under section 51 of the DPA. The exemption provided under section 52 (ii) is applicable to the extent that the disclosure made to the police by Respondent 2 is required for on-going or prospective legal proceedings. This is to be distinguished from the illegal disclosure made to the press as the evidence shows. The information is sensitive as they concern the complainants' involvement in the alleged commission of an offence (fraud) as per section 2 of the DPA and none of the exceptions under section 25 are applicable in this context.

EU Article 29 Data Protection Working party opinion 4/2007 on the concept of personal data at page 6, last paragraph, stated as follows:-

"*The term "personal data" includes information ....regarding whatever types of activity is undertaken by the individual, like that concerning working relations or the economic or social behaviour of the individual. It includes therefore information on individuals, regardless of the position or capacity of those persons (as consumer, patient, employee, customer,etc).*

Judgment of the European Court of Human Rights in the case Amann v Switzerland of 16.2.2000, §65, it was stated: *"[...] the term "private life" must not be interpreted restrictively.*

In particular, respect for private life comprises the right to establish and develop relationships with other human beings; furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life" (see the Niemietz v. Germany judgment of 16 December 1992, Series A no. 251-B, pp. 33-34, § 29).

Judgment of the European Court of Justice C-101/2001of 6.11.2003 (Lindqvist), §24, it was stated: "*The term personal data used (...) covers, according to the definition (...), any information relating to an identified or identifiable natural person. The term undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies*".

It is clear from the above judgments whose principles are applicable in our local context given the similarities between our DPA and the international instruments governing the reasoning applied in these judgments - that we are here dealing with personal sensitive information. Since the DPA caters for the breach of its provisions as criminal offences, the standard of proof in our law used for offences is naturally the criminal standard, that is, the burden of proof that lies on the prosecution side (the complainant) is one beyond reasonable doubt and the burden of proof for the respondent is balance of probabilities. Although the decision of the Commissioner, in case of prosecution is referred to the Commissioner of Police for subsequent procedures required for the case to be brought to court, it has to take into consideration our penal system and not civil principles which are not applicable in the context. The decision of the Commissioner further concentrates only on potential breaches of the DPA as revealed by the facts and excludes all irrelevant considerations to data protection principles.

In the case of Nikolaou v. Commission (12.9.2007 - T-259/03- ECJ), it was held that:-

"an organisation had disclosed certain information about its investigation concerning the applicant: a leak of information to a journalist; its annual report with information about the investigation; and its press statement. The applicant had requested access to the file and the final case report. The Court concluded that a staff member leaked information (including personal data) to a journalist, which were published, and the organisation's press release confirmed the veracity of facts (including personal data) that had been mentioned in several press articles.

The information published in the press release was personal data, since the data subject was easily identifiable, under the circumstances. The fact that the applicant was not named did not protect her anonymity. The leak (unauthorised transmission of personal data to a journalist by

someone inside the organisation) and the publication of a press release each constitute processing of personal data.

The leak constitutes unlawful processing because it was not authorised by the data subject. The organisation is best placed to prove how the leak occurred and that the Director of the organisation did not violate his obligations. In the absence of such proof, he must be held responsible. No concrete showing was made of an internal system of control to prevent leaks or that the information in question had been treated in a manner that would guarantee its confidentiality.

Publication of the press release was not lawful because the public did not need to know the information published in the press release at the time of its publication, before the competent authorities had decided whether to undertake judicial, disciplinary or financial follow-up."

In the light of the above, it is clearly established that there has been a breach of section 26 (1) (b) of the DPA by Respondent 2 in his capacity as member of the Board of Directors of the organisation and thus as a data controller who decides together with other persons of the uses to be put to the personal information contained in the report, he failed to ensure that the data in his possession have not been used or disclosed in any manner incompatible with the purposes for which such data has been collected and processed. The press statements made by him and the production and distribution of the pamphlet are evidence of the fact that the confidential internal audit report so far as personal information contained therein are concerned have unlawfully been communicated to the press and commented thereon before the police enquiry has been successfully completed, as initiated by him. Once a case is reported to the police for example, it is then the responsibility of the relevant competent authorities including the court to provide its findings and Respondent 2 had the duty to await this conclusion and not to preempt the outcome. Complainants have been unfairly tried in the press and pronounced as guilty which is not the proper forum based upon the contents of the internal audit report.

With regard to the responsibility of organisation, it is also clear that the internal audit report was brought to the attention of the board members for the purpose of confidentially apprising them of its contents and not meant to be used otherwise in an incompatible way. Therefore, no evidence has been adduced by complainants as regards whether the chairman and the other organisation board members have condoned or approved the leakage caused by Respondent 2 who himself is part of organisation as board member. However, since no *"concrete showing was made of an internal system of control to prevent leaks or that the information in question had been treated in a manner that would guarantee its confidentiality*", as stated in the case of *Nikolaou* above, by the organisation, I am of the view that the organisation has failed to prove

on a balance of probabilities as Respondent that there has been no breach of sections 27(1) & (2) of the DPA.

Therefore, in my view, the case for prosecution has been established beyond reasonable doubt and prosecution is thus advised against Respondent 1 for breach of sections 27(1) & (2) and 61 of the DPA and against Respondent 2 for breach of sections 25 (1), 26(1) (b), 29(1) and 61 of the DPA. Complainants never gave their express consent for their personal data to be published nor made them public. The matter is thus referred to the Police under section 20 of the DPA.

As regards the different press institutions involved in this case, they are reminded that section 49 of the DPA is to be used with great caution- journalistic processing of personal information should only be justified when there is a reasonable belief that the publication would be in the public interest and compliance with the DPA would be incompatible with the journalistic purposes claimed. The test is not a simple one. Complainants may wish to explore other available legal avenues against the press such as civil proceedings.

Mrs Drudeisha Madhub

Data Protection Commissioner

Data Protection Office

Prime Minister's Office

4th floor, Emmanuel Anquetil Building, Port Louis

12.05.14.