



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

EA and TA,

Complainant,

-versus-

NPC Case No. 17-018

*For: Violation of Section 25 (b) of the
Data Privacy Act of 2012*

EJ, EE and HC,

Respondents.

x-----x

DECISION

For consideration of the Commission is the complaint filed by Complainants EA and TA against Respondents EJ, EE and HC for Violation of Section 25(b) of the Data Privacy Act of 2012 (DPA).¹

Relevant Facts

Complainants allege that:

1. On 07 April 2017, Respondents EJ and HC filed a case against Complainant TA for Falsification of Public Documents docketed as NPS No. VI-10-INV-17D-00915 before the Office of the City Prosecutor of Iloilo City;
 - a. The case involved the alleged falsification of the two birth certificates of CEA and CTA, the sons of TA.

¹ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012]

- b. EJ alleged that TA falsified the entries in the certificates of live birth stating that the Complainants were married on December in California, USA.
 - c. EJ also submitted before the Office of the City Prosecutor of Iloilo City the Certificate of Marriage² between Complainant EA and a certain MS and Certificates of No Marriage (CENOMAR)³ of both complainants.
2. Respondents were neither authorized to obtain nor access any of the mentioned documents, as well as the personal information contained therein.
 3. Respondent EE obtained said documents containing sensitive personal information under the order of her employer, EJ. They resorted to underhanded means in obtaining these documents.
 4. The acts of Respondents endanger the sanctity and privacy of the Complainants and the public at large.⁴

Complainants allege that Respondents committed unauthorized processing of sensitive personal information prohibited under the DPA. Complainants argue that the documents containing sensitive personal information were obtained without their consent and without authority under the DPA or any existing law.

On 31 August 2017, Complainants submitted their Supplemental Complaint reiterating the points already raised in their Complaint-Affidavit.⁵

On 18 September 2017, Respondents EJ and EE, filed their Comment, where they raised the following arguments:

² Records, p. 40.

³ *Id.*, at pp. 12 and 15.

⁴ *Id.*, at pp. 1-3.

⁵ *Id.*, at pp. 56-58.

1. The Data Privacy Act of 2012 does not apply to them because it only covers natural and juridical persons involved in data processing;
2. The act of reporting the matter as to the true and factual marital status of the complainants to the proper authorities is not considered within the definition of “processing of personal sensitive [sic] information” no matter how expansive the definition of the term;
3. The marital status of Complainants are not personal or sensitive personal information because they are there for everybody to know. They are to be considered as “public records” as they are readily available from the public registry. Complainants are even fostering in all their complaints, pleadings and allegations that they are married, and they have legitimate children; and
4. Assuming that processing was done with the sensitive personal information of Complainants, it was made for a legitimate purpose of filing a criminal complaint of falsification.⁶

Respondents EJ and EE submitted their Supplemental Comment containing substantially the points they previously raised in their Comment.

On 17 November 2017, Complainants personally filed before the Commission their Reply refuting the arguments of Respondents stating that:

1. Personal sensitive information, as defined under the Data Privacy Act, is privileged and confidential and prohibits its processing except in certain circumstances, under Section 13 of R.A. 10173. Complainants allege that the act of respondents does not fall within the exceptions in processing sensitive personal information.
2. Neither EJ, EE, nor their authorized agents were the data subjects concerned in the documents requested. Therefore, they have no authority to access or use the personal sensitive information in the subject documents

⁶ *Id.*, at pp. 186-193.

pertaining to the Complainants and their children. It is clear from the Data Privacy Act that these can only be obtained by the data subject themselves or their authorized representatives.⁷

On 10 January 2018, a Discovery Conference was held⁸ where all the parties appeared except for Espinosa. During the conference, it was made known to the Commission that Respondent HC is the sister of Complainant TA.

According to EJ, they requested the subject documents from Philippine Statistics Authority (PSA) because TA filed a petition for guardianship proceedings over her mother who was EJ's client. EJ explained that the documents were obtained to determine the moral fitness of TA as the guardian of his client.⁹

Further, he also said that the documents were obtained sometime in September 2016, before PSA issued in 2017 the guidelines limiting the release of those kinds of documents only to specified authorized persons.¹⁰ He alleged that after obtaining the documents, he learned of the marital circumstances of TA. This incident prompted him to file a complaint for falsification against her.

Based on the documents submitted and the proceedings held, it appears that there were other pending cases between the parties and that the conflict between them started when HC, by virtue of a Special Power of Attorney, sold some of the properties of their mother. EJ was the one who notarized all the legal documents pertaining to the sale. When Complainants discovered those transactions, the parties started filing different cases against each other, including the present complaint. Respondents used the subject documents in the guardianship proceedings and in the criminal complaint against Complainants.¹¹

ISSUE

⁷ *Id.*, at pp. 266-275

⁸ *Id.*, p. 304.

⁹ *Id.*, p. 310. Transcript of Discovery Hearing on 10 January 2018.

¹⁰ *Id.*

¹¹ *Id.*, at pp. 4-20. Annex of the Complaint-Affidavit.

The sole issue to be determined in this case is whether the Respondents violated Section 25 (b) of the DPA in processing the Complainant's personal data for the purposes described above.

DISCUSSION

In determining whether a violation of Section 25(b) of the DPA occurred, three elements must be established with substantial evidence:

1. The accused processed the information of the data subject;
2. The information processed was personal information or sensitive personal information;
3. That the processing was done without the consent of the data subject, or without being authorized under this act or any existing law.

As to the first element, the DPA provides a definition of processing as "any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data."¹² Simply stated, processing refers to any use of personal data at any stage of the data life cycle.

In this case, Respondents requested and consequently obtained the subject documents from PSA in order to look into the personal circumstances of Complainant TA and, in view of the petition for guardianship proceedings she filed for their mother, to oppose to TA's moral fitness as such guardian.

Respondent EJ also used the same documents in filing the criminal complaint docketed as NPS No. VI-10-INV-17D-00915 before the Office of the City Prosecutor of Iloilo City. The documents, containing the personal and sensitive personal information of Complainants were annexed to the criminal complaint to support his allegations in that case.

Given these, Respondents' actions of collecting, storing, and using the sensitive personal information of Complainants as evidence

¹² Data Privacy Act of 2012, § 3(j).

to support their allegations in the criminal complaint in NPS No. VI-10-INV-17D-00915 is considered processing of sensitive personal information.

Any misconception about “processing” being limited to digital means should be dispelled. The DPA covers not just the processing of digital data but any processing of personal information whether it is in a digital or paper form. The DPA does not distinguish.

As to the second element, the information subject of this case is sensitive personal information. Under the DPA, sensitive personal information refers to information:

1. About an individual’s race, ethnic origin, **marital status**, age, color, and religious, philosophical or political affiliations;
2. About an individual’s health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
3. Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
4. Specifically established by an executive order or an act of Congress to be kept classified.¹³

Contrary to the allegations of Respondents that “[t]he information as to the marital status of Complainants are there for everybody to know, it is not personal nor sensitive, since marital status of a person is public information,”¹⁴ marital status is specifically included in the enumeration of what is considered sensitive personal information under the DPA.

¹³ Data Privacy Act of 2012, § 3(l). Emphasis supplied.

¹⁴ Records, p. 251.

It is a misconception that publicly available personal data can be further used or disclosed for any purpose whatsoever without regulation. Personal data does not lose the protection afforded by the DPA simply because it has been made public or is publicly accessible.¹⁵

In this case, the fact that Complainants announce their status in public does not change the nature of this information as sensitive personal information. The law specifically enumerates what can be considered as sensitive personal information based on the potential risk posed by its processing to the data subject, and the enhanced protection needed to avert it. Under the Act, the rule is that the processing of the enumerated sensitive personal information is prohibited unless one of the grounds for lawful processing of such sensitive personal information is present.¹⁶

With regard to the third element, Section 13 of the Act expressly prohibits the processing of sensitive personal information, except in the following cases:

“xxx

- f. The processing concerns such personal information as is **necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims**, or when provided to government or public authority (Emphasis supplied).”

During the Discovery Conference, it was repeatedly brought to the attention of the Commission that the Complainants and Respondents were already opposing parties in a guardianship proceeding even before Respondents filed the criminal complaint for Falsification against Complainants. In the guardianship proceeding, TA is the petitioner while EJ is the counsel of the ward subject of the proceedings.

EJ insists that the relevant documents were obtained while there was a pending case between them. He allegedly processed the sensitive personal information of Complainants to protect the interest of his client in the guardianship proceeding before the Regional Trial

¹⁵ See, Data Privacy Act of 2012, § 4; IRR §§ 4 & 5.

¹⁶ Data Privacy Act of 2012, § 13.

Court of Roxas City, Iloilo, Branch 14.¹⁷ The Respondents, however, failed to substantiate this allegation.

On this matter, it must be clarified that the Data Privacy Act makes a distinction between the three instances where Section 13(f) is applicable, namely: (a) The processing is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings; (b) The processing is necessary for the establishment, exercise or defense of legal claims; or (c) The processing concerns personal information that is provided to government or public authority.

In this case, while no evidence was submitted to establish that the subject documents were presented in the guardianship proceedings, it is not, however, disputed that the Respondents used the subject documents to build a case for falsification of public documents against Complainants. This falls squarely under the instance of “processing as necessary for the establishment of legal claims” which does not require an existing court proceeding. To require a court proceeding for the application of Section 13(f) to this instance would not only be to disregard the distinction provided in the law but the clear letter of the law as well. After all, the very idea of “establishment ... of legal claims” presupposes that there is still no pending case since a case will only be filed once the required legal claims have already been established.

In addition, the use of the qualifier “necessary” in the law should be understood to apply not just to the “protection of lawful rights and interests of...persons in court proceedings” but also to the “establishment... of legal claims.”

The DPA should not be seen as curtailing the practice of law in litigation. Considering that it is almost impossible for Congress to determine beforehand what specific data is “necessary” or may or may not be collected by lawyers for purposes of building a case, applying the qualifier “necessary” to the second instance in Section 13(f) therefore, serves to limit the potentially broad concept of “establishment of legal claims” consistent with the general principles of legitimate purpose and proportionality.

¹⁷ Records. p. 6.

As regards legitimate purpose, the Implementing Rules and Regulations (IRR) of the Data Privacy Act provides that the processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.¹⁸ This means that the processing done for the establishment of a legal claim should not in any manner be outside the limitations provided by law. The DPA is neither a tool to prevent the discovery of a crime nor a means to hinder legitimate proceedings.

In this case, the collection of the subject documents was in view of the falsification case that was eventually filed with the Regional Trial Court of Roxas City, Iloilo. The processing of the documents for this cannot be considered as wrongful or illegal.

This is all the more true since the subject documents were obtained by the respondents from the Philippine Statistics Authority (PSA) before the PSA limited the authorized persons who can request for copies of Certificates of Birth, Certificates of Marriage and Certificates of Death when it issued Office Memorandum No. 2017-050¹⁹ on 17 April 2017 and the Memorandum Circular No. 2017-09²⁰ on 19 June 2017, thus:

1. 28 October 2016 - Certificate of Live Birth of CEA;
2. 25 October 2016 - Certificate of Live Birth of CTA;
3. 25 October 2016 - The Marriage Certificate of EA and MS with annotation of Final Judgment of Nullity of Marriage under Article 36 of the Family Code;
4. 30 October 2016 - Certificate of No Marriage (CENOMAR) of TA; and
5. 30 September 2016 - CENOMAR of EA.

¹⁸ Implementing Rules and Regulations of the Data Privacy Act of 2012 (hereinafter, "IRR"), § 18(b).

¹⁹ Records. p. 270.

²⁰ Records. p. 276.

It should be stressed, however, that having a legitimate purpose or some other lawful criteria to process does not result in PSA being legally obliged to grant such request. A person requesting for certain information from an administrative agency remains to be subject to that agency's guidelines for the release of such information. In this case, had Respondents requested for the abovementioned certificates after the PSA issued its guidelines, they would have been obliged to comply with such despite having complied with the requirements of the DPA on lawful criteria for processing.

Aside from legitimate purpose, the qualifier "necessary" also pertains to the general privacy principle of proportionality. Under the IRR, the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed **only if the purpose of the processing could not reasonably be fulfilled by other means.**²¹

The proportionality principle, as manifested in the qualifier "necessary" serves as a sufficient test in determining whether the processing is justified in relation to the declared purpose.

In this case, considering that the documents were used in the falsification case and absent any showing that its use was unjustified, it cannot therefore be said that the processing done by Respondents was not necessary.

While the processing of sensitive personal information is expressly prohibited under Section 13 of the Act, the processing made on the sensitive personal information of Complainants falls under one of the exceptions thereto. The Commission finds that the third element is not present in this case. Respondents did not commit unauthorized processing of sensitive personal information under Section 25 (b) of the Data Privacy Act of 2012.

While we find that the Respondent did not violate Section 25 (b) of the Data Privacy Act of 2012, this does not, however, preclude any civil, criminal or administrative liability, if any, on the part of the Respondents arising from other laws.

²¹ IRR, § 18(c), emphasis supplied.

DISPOSITIVE

WHEREFORE, the foregoing considered, this Commission finds that Respondent did not violate Section 25(b) of the Data Privacy Act of 2012 on unauthorized access of sensitive personal information.

This is without prejudice to the filing of appropriate civil, criminal or administrative cases against the respondents before any other forum or tribunal, if any.

SO ORDERED.

Pasay City, 15 July 2019.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Concurring:

Sgd.
IVY D. PATDU
Deputy Privacy Commissioner

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

COPY FURNISHED:

EA

TA

EJ

EE

HC

ENFORCEMENT DIVISION

*Legal and Enforcement Office
National Privacy Commission
5th Floor West Banquet Hall, Delegation Bldg.
PICC Complex, 1307 Manila*