Republic of the Philippines
NATIONAL PRIVACY COMMISSION

**MNLC, INC.** represented by **IKP,**

*Complainant,*

-versus-

**NPC Case No. 19-528**
**(**Formerly CID Case No. 19-G-528)
*For: Violation of Section 13, in relation to Section 25(b) of the Data Privacy Act*

**PXXX CORPORATION, RCM and AD,**

*Respondent.*

x----------x

# DECISION

***AGUIRRE*, D.P.C.:**

Before this Commission is a Complaint filed by Complainant MNLC, Inc. (MNLCI) against Respondents PXXX Corporation, RCCM, and AD, for an alleged violation of Republic Act No. 10173 ("Data Privacy Act").

## The Facts

Complainant MNLC, Inc. (MNLCI), represented by its Head Elder IKP, is a religious corporation composed mostly of Koreans and their families who practice Christianity in the Philippines. The religious officers and church members of the Complainant regularly gather during Sundays in its place of worship located at the 3rd Floor of MXXX Building being managed by Respondents. For the past nine (9) years, Complainant has owned all the units on the third floor of the building.[1]

Sometime in March 2019, Respondent PXXX Corporation (Respondent Corporation) started implementing security measures in the building that required the Complainant to submit Philippine

[1] Records, pp. 1-7 dated 19 July 2019.

government-issued identification cards (IDs) of their church members.[2]

Respondent RCM, OIC-Administration Department and Marketing Manager of MNLCI, sent a letter to Complainant, through PMH, reminding the latter that the implementation of such security measures will start on 05 May 2019.[3] He also sent a letter dated 06 May 2019 to all tenants and unit owners of the building informing them about the strict enforcement of "No ID, No Entry" policy in the building.[4]

On 16 May 2019, the Complainant, through its counsel, reached out to the Respondents to clarify matters concerning the implementation of said new policy. However, Complainant's counsel and Respondents failed to meet and talk about the issues on the newly implemented security measures.[5]

On the same day, Respondent AD, Legal and Corporate External Affairs Head of MNLCI, sent a letter to Complainant reiterating the submission of original Philippine government-issued or any valid IDs from its church members on weekdays from 10:00A.M. to 12:00P.M. supposedly for validation purposes. Respondent also stated that the IDs provided by Complainant to its church members are denied and are not to be acknowledged by the security personnel of the building.[6]

Complainant sent more letters to the Respondents requesting for the basis in requiring the Complainant's church members to submit their IDs. Specifically, the Complainant asked for the following: (1) a copy of the House Rules and Regulations of the Respondent Corporation; (2) reports of the crimes allegedly committed in the building; and (3) reports to the police concerning these crimes.[7]

RCM insisted in a letter dated 26 May 2019 that the church members of Complainant should submit their original passports, valid IDs bearing their Philippine residence addresses, and colored ID pictures for the production of their respective IDs to be used in

[2] Fact-Finding Report dated 14 October 2020, at p. 1.
[3] *Supra* note 1, at 29 dated 30 April 2019.
[4] *Id.*, at 30 dated 06 May 2019.
[5] *Id.*, at 3.
[6] *Id.*, at 33 to 35 dated 16 May 2019.
[7] *Id.*, at 42 dated 26 May 2019.

entering the premises of the building.[8] However, Complainant received another letter dated 31 May 2019 from the counsel of Respondent Corporation stating that the Complainant will be the one to provide the IDs for its members.[9]

Since the letter of RCM contradicts the statements in the letter of Respondent Corporation's counsel, Complainant tried to secure a copy of the building rules where the implemented security measures are based upon.[10] Up to the filing of the Complaint, Complainant was unable to secure a copy of the same.[11]

Upon the surrender of the passports and valid IDs of the Complainant's church members, employees of the Respondent Corporation took photos of their passports and valid IDs using their mobile phones.[12] The employees utilized these identification documents to produce another ID to be paid by the church members.[13]

Complainant's church members had no recourse but to submit their IDs containing their addresses and other personal data in order to avoid being harassed during frisking. Some of these members were forced to give their passports and IDs in order to practice their religion peacefully.[14]

## Proceedings

The case was called for a summary hearing on 02 August 2019 for Complainant's application for a temporary ban where the parties were also required to submit the judicial affidavits of their witnesses in accordance with Sections 3 and 4 of A.M. No. 12-8-8-SC dated 4 September 2012 (Judicial Affidavit Rule).[15]

[8] *Id.*, at 42 dated 26 May 2019.
[9] *Id.*, at 40 to 41 dated 31 May 2019.
[10] *Id.*, at 51 to 53 dated 03 June 2019.
[11] *Supra* note 2, at p. 2.
[12] *Supra* note 1, at 61.
[13] *Id.*, at 5.
[14] *Supra* note 2, at p. 2.
[15] *Supra* note 1, at 64 and 65.

Respondent's counsel of record filed a Formal Entry of Appearance with Motion for Resetting and Extension of Time to File Responsive Pleading, asking for the resetting of the summary hearing to 16 August 2019 in order to have additional time to prepare the necessary pleadings for the summary hearing.[16]

Both parties and their respective counsels appeared during the scheduled summary hearing on 02 August 2019. However, Respondents' representative and counsel, by way of special appearance, only arrived after the hearing was already adjourned. Complainant submitted the judicial affidavits of its witnesses, namely, IKP, HCM, GSP, and HHJ. Considering that it was the first setting for the summary hearing and the reasons of the Respondents' counsel in the motion were reasonable, the motion for resetting was granted. The parties were ordered to appear on 09 and 16 August 2019.[17]

The counsels of both parties appeared for the summary hearing on 09 August 2019. The parties identified the witnesses to be presented for the summary hearing. Complainant's counsel manifested that there was a failure on its part to attach the Secretary's Certificate mentioned and to attach as Annex "A-1" in the judicial affidavit of its witness IKP due to inadvertence. Respondents were given a period of five (5) days to make the necessary changes on the judicial affidavits of their witnesses considering that they raised the issue of Complainant's lack of legal personality.[18]

Parties presented their testimonial and documentary evidence during the last scheduled summary hearing on 16 August 2019. Complainant presented its witnesses, namely, IKP, HCM, GSP, and HHJ. Meanwhile, Respondents presented their witness, AD. All the witnesses identified their judicial affidavits and adopted the same as their direct testimonies. The presentation of evidence for both parties was then terminated. Respondents were required to submit within four (4) days the building's rules and regulations and the incident reports mentioned during the presentation of witnesses. Respondents asked for five (5) days to submit written

[16] *Id.*, at 66 to 68.
[17] *Id.*, at 69, 157 and 158.
[18] *Id.*, at 159, 179 and 180.

manifestation. Complainant also asked for the same period to file a comment to the manifestation of the Respondents.[19]

On 20 August 2019, Respondents filed a Memorandum as an answer to Complainant's application for a temporary ban on the processing of its church members' personal information. Respondents discussed the issues they believed were for resolution. First, Respondents submitted the issue that the Commission should rule on which legal authority between the Data Privacy Act and the NPC Rules of Procedure should be relied upon. Second, Respondents also raised the issue whether the alleged violation in the complaint is detrimental to national security and public interest. Third, Respondents questioned the legal personality of Complainant because it cannot be considered as data subject whose personal information is being processed. Lastly, Respondents claimed that Complainant failed to exhaust administrative remedies because the correspondences sent by the latter's counsel lacked the required special power of attorney or the Secretary's Certificate.[20]

The Commission, through the investigating officer, issued an Order dated 11 September 2019 granting the temporary ban on the processing of personal data against Respondent Corporation. The ban covered: (1) the processing of personal data of Complainant's church members who have not yet provided their identification documents to Respondents for validation; and (2) the requirement for the use of Respondent corporation-issued IDs for the Complainant's church members who have already submitted their passports and IDs.[21]

In the same Order, Respondent Corporation was also directed to (1) return to Complainant's church members all the copies of their passports and valid IDs; (2) delete or dispose all copies of the passports and valid IDs, digital or otherwise; and (3) to allow Complainant to provide IDs for their church members and officers bearing only their photos and English names. Further, Respondents were also required to submit an affidavit of compliance stating that the personal data of Complainant's church

[19] *Supra* note 2, at p. 3.
[20] *Supra* note 1, at 244 to 253.
[21] *Id.*, at 276 to 279.

members are no longer kept independently in any of Respondent Corporation's records.[22]

On 25 September 2019, Respondents filed a Motion for Reconsideration of the Order imposing a temporary ban on its processing of personal data of Complainant's church members. The motion is premised on the ground that the complaint is not imbued with public interest supposedly because Complainant's church members belong to a particular and specified class composed mostly of foreign individuals. As such, according to Respondents, "they cannot be considered public in general for the protection against public interest to apply."[23] Respondents further argued that the temporary ban should not have been issued in the first place because the acts complained of are not considered imbued with public interest.[24]

Respondents also filed an Addendum to the Motion for Reconsideration. The Addendum discussed that Complainant provided a clear, explicit and emphatic consent in using the Respondent corporation-issued ID.[25]

On 11 October 2019, both parties and their counsels attended the discovery conference. Both parties manifested that they were not seeking any additional information or documents from each other. The Complainant and Respondents also filed a Manifestation and Counter-Manifestation, respectively, as to whether the directives in the Order dated 11 September 2019 were stayed by the Respondents' Motion for Reconsideration. Respondents were ordered to file their Responsive Comment to the complaint. Complainant was also ordered to file its reply to the comment.[26]

On 28 October 2019, Respondents filed a Responsive Comment to the Complaint. They raised similar issues discussed in the memorandum they previously submitted. First, Respondents assailed the legal personality of Complainant as it is not considered a data subject because it is a corporate or artificial being only existing in contemplation of law. They pointed out that the individual members of Complainant have not executed any

[22] *Ibid*.
[23] *Id., at* 287.
[24] *Id*., at 285 to 292.
[25] *Id*., at 293 to 298.
[26] *Id*., at 332 to 333.

authorization designating Complainant or any of its witnesses to represent them in the proceedings before the Commission. Second, Respondents also allege that Complainant failed to exhaust administrative remedies. They argue that, although there were several correspondences between Complainant's counsel, Abellera and Calica Law Offices, and Respondents, there was no special power of attorney or Secretary's Certificate showing that Complainant's counsel is also authorized to represent the individual members of Complainant. Third, Respondents claim that they have observed the general data privacy principles of transparency, legal purpose, and proportionality in processing the personal information of complainant's church members.[27]

Respondents also filed an Addendum to the Responsive Comment. They added that processing the personal information of Complainant's church members was necessary to achieve lawful and non-commercial objectives considering that Respondent Corporation undertook heightened security measures in view of the crimes against properties committed to their tenants inside the building.[28]

On 14 November 2019, Complainant manifested that the contents of Respondents' Comment are a mere rehash of their previous arguments as discussed during the proceedings on the issuance of a temporary ban. Complainant also prayed for indemnification, destruction of its church members' personal data processed by Respondents, and a recommendation to prosecute Respondents for violation of Section 13 in relation to Section 25(b) of the Data Privacy Act.[29]

On 18 November 2019, the Commission issued a Resolution denying the Motion for Reconsideration of the Order dated 11 September 2019 issuing a temporary ban on processing against Respondents. The Commission also required Respondents to submit an affidavit of compliance showing that they have complied with the Commission's order to: (1) return to complainant's church members all the copies of their passports and valid IDs; (2) delete or dispose all copies of the passports and valid IDs, digital or otherwise; and (3) to allow complainant to

[27] *Id.*, at 335 to 351.
[28] *Id.*, at 352 to 359.
[29] *Id.*, at 361 to 362.

provide IDs for their church members and officers bearing only their photos and English names.[30]

Thereafter, Complainant filed a Manifestation and Motion dated 03 February 2020 stating that Respondent Corporation continues to require Complainant to use only the Respondent Corporation-issued IDs to gain entrance to the building, and claimed that such act was in defiance of this Commission's Order dated 11 September 2019 and Resolution dated 18 November 2019. Complainant also manifested that Respondent has not yet submitted an affidavit of compliance.

Given this, Respondents were ordered to show cause and explain why it should not be held in contempt for disregarding this Commission's Order.[31]

On 27 February 2020, Respondents filed a Manifestation and Motion (with notice of change of office address). Respondents moved that the pending show cause Order's resolution be deferred considering that the parties were on the verge of signing a compromise agreement.[32]

This Commission denied the Motion seeking to defer its compliance with the show cause order explaining that the possible signing of a compromise agreement and the issue of failing to comply with this Commission's Order are completely different matters. Respondents were given a final opportunity to submit their explanation to the show cause order.[33]

On 03 June 2020, Complainant manifested that it sent a letter dated 06 March 2020 to the Respondents, terminating all efforts for settlement. As such, it urged the Commission to seek Respondents' compliance with the Orders dated 11 September 2019 and 18 November 2019.[34]

On 09 June 2020, the Respondents filed their Compliance *ad Cautelam*. In the Joint Affidavit of Compliance executed by Respondents AD and RCM, they claim that Respondent Corporation had ceased from processing the personal information

[30] *Id.*, at 369 to 376.
[31] Order dated 14 February 2020.
[32] *Supra* note 2, at pp. 5-6.
[33] Order dated 03 March 2020.
[34] Manifestation dated 09 March 2020.

of Complainant's church members by stopping the issuance of IDs to them. They also mentioned that all copies of passports, other valid IDs and personal data digitally stored or otherwise from Complainant's church members were completely deleted and disposed. They also stated that the Respondent Corporation no longer required Complainant's church members to use the Respondent Corporation's-issued IDs.[35]

On 17 August 2020, Complainant filed a Motion to Resolve asking that the case already be considered submitted for resolution.[36]

## Issues

The issues in this case are:

1. Whether this Commission validly acquired jurisdiction over this case;
2. Whether the Complaint should be dismissed on the ground of non-exhaustion of remedies under NPC Circular 16-04;
3. Whether Respondent obtained valid consent from Complainant to collect and process personal and sensitive personal information from their members;
4. Whether Respondent had a legitimate interest to collect and process personal and sensitive personal information from Complainant's members;
5. Whether Respondent complied with the principle of proportionality in collecting and processing personal and sensitive personal information from Complainant's members;
6. Whether Respondent is liable for unauthorized processing of personal and sensitive personal information of Complainant's members;
7. Whether the Complainant is entitled to damages; and
8. Whether the Compliance Ad Cautelam submitted by Respondents is sufficient in relation to the Order dated 03 March 2020.

## Discussion

*This Commission validly acquired jurisdiction over this case*

[35] Joint Affidavit of Compliance dated 08 June 2020.
[36] Motion to Resolve dated 26 June 2020.

Respondents argue that this Commission has not validly acquired jurisdiction over this case because Complainant has no personality to file the complaint supposedly because the real party in interest, the individual members of MNLCI, "have not executed any authorization authorizing MNLC or IKP, GSP and HCM to represent them in this proceedings (sic)."[37] On the basis of this, Respondents further argue that "IKP, GSP and HCM are testifying as mere representatives/witnesses and not as complainants. It is therefore submitted that, for this Commission to have jurisdiction, a formal complaint must be filed by a data subject."[38]

The important consideration in determining whether this Commission validly acquired jurisdiction over a case is whether the allegations, assuming they were true, show that a privacy violation was committed against a data subject.

In this case, IKP, the Head Elder of MNLC, Inc., alleged in his Complaint-Affidavit that Respondents committed acts violative of his privacy rights. The fact that he and the other church members, who executed affidavits in support of the Complaint-Affidavit, also sought to represent the other members of MNLCI does not change their status as affected data subjects.

Whether IKP and the others were testifying as mere representatives or witnesses and not as complainants or whether each and every single member of MNLCI should have issued individual authorizations is of no moment. Strict adherence to the technicalities of NPC Circular No. 16-04 or the NPC Rules of Procedure ("Rules") may be dispensed with following Section 33 of the same Rules which provide for a liberal interpretation "in a manner mindful of the rights and interests of the person about whom personal data is processed."[39] As the Supreme Court held in *Heirs of Amada Zaulda v. Zaulda*,[40] technicalities may be dispensed with if it impedes the attainment of justice, thus:

> What should guide judicial action is the principle that a party-litigant should be given the fullest opportunity to establish the merits of his complaint or defense rather than for him to lose

[37] Memorandum dated 20 August 2019.
[38] *Id.*
[39] *FGP v. Maersk*, NPC Case No. 18-038, 21 May 2020.
[40] G.R. No. 201234, March 17, 2014.

> life, liberty, honor, or property on technicalities. The rules of procedure should be viewed as mere tools designed to facilitate the attainment of justice. Their strict and rigid application, which would result in technicalities that tend to frustrate rather than promote substantial justice, must always be eschewed.[41]

As to the supposed privacy violations, it should also be noted that Respondents themselves admitted that the processing at issue in this case involved the personal data of all the members of MNLCI. In their Addendum to the Motion for Reconsideration, Respondents argue that the emails of IKP and the other members of MNLCI supposedly show that they can validly process the personal data of the entire MNLCI congregation on the basis of consent, thus:

> 1. MNLC (MNLC) by means of electronic message or Email dated June 26, 2019 personally and knowledgeably notified and confirmed herein respondents that MNLC's (sic) **including all MNLCI members pastors and elders** will use MXXX ID thus **manifesting a clear, explicit and emphatic consent of the entire congregation**…
> 2. … Also, as it can be garnered from the letter is unequivocal consent to **scan MNLCI Members government issued identification**…[42]

Having admitted the allegations in the Complaint relating to the processing of the personal data of all the members of MNLCI's congregation, albeit supposedly on the basis of consent, Respondents cannot now claim that this Commission did not acquire jurisdiction. The determination of the validity of the processing carried out by Respondents, including whether the basis relied upon to process is proper, is precisely within the mandate of this Commission.

In addition, Respondents mistakenly assume that the Commission can only acquire jurisdiction on a matter affecting any personal information if a formal complaint is filed by a data subject. Respondents fail to consider, however, that the Commission is fully empowered to investigate, on its own initiative,

---

[41] *Ibid.*

[42] *Supra* note 1, at 311-312. Emphasis supplied.

circumstances surrounding a possibly serious privacy violation or personal data breach.[43] The allegations in the Complaint raise potentially serious privacy violations that require this Commission to take such further action on the matter as may be necessary, after having been informed of the same.

*The Complaint should not be dismissed on the basis of non-exhaustion of remedies*

Respondents claim that Complainant failed to exhaust administrative remedies because the correspondences sent by the latter's counsel lacked the required special power of attorney or the Secretary's Certificate.[44]

NPC Circular No. 16-04 provide for the rule on exhaustion of remedies, thus:

> Section 4. Exhaustion of remedies. No complaint shall be entertained unless:
>
> xxx
>
> a. the complainant has informed, in writing, the personal information controller or concerned entity of the privacy violation or personal data breach to allow for appropriate action on the same; [45]

As this Commission has ruled in a previous Decision,[46] this rule was intended to prevent a deluge of vexatious complaints from those who waited for a long period of time to pass before deciding to lodge a complaint with the NPC, unduly clogging its dockets. Notably, however, the same Section provides that the Commission has the discretion to waive any of the requirements upon good cause shown, or if the complaint involves a serious violation or breach of the Data Privacy Act, taking into account the risk of harm to Complainant.

---

[43] *Supra* note 2, at p. 6.
[44] *Supra,* note 20.
[45] Section 4, Rule II, NPC Circular 16-04. Dated 15 December 2016.
[46] NPC Case No. 18-083, dated 21 May 2020.

That Decision cited the Supreme Court in stating thus:

> The Court has allowed some meritorious cases to proceed despite inherent procedural defects and lapses. This is in keeping with the principle that rules of procedure are mere tools designed to facilitate the attainment of justice and that strict and rigid application of rules which would result in technicalities that tend to frustrate rather than promote substantial justice must always be avoided. It is a far better and more prudent cause of action for the court to excuse a technical lapse and afford the parties a review of the case to attain the ends of justice, rather than dispose of the case on technicality and cause grave injustice to the parties, giving a false impression of speedy disposal of cases while actually resulting in more delay, if not a miscarriage of justice.[47]

The Rules include, as a ground for the Commission to waive any of the requirements, instances when the complaint involves a serious violation or breach of the Data Privacy Act. In this case, the Complaint-Affidavit contains allegations such as:

> 23. The series of acts of harassment by PXXX to force MNLCI's members to comply and submit their passports and ID's is a violation of Section 13. There could never be consent if the MNLCI member is harassed or, at the very least, inconvenienced by long lines or body frisking to force him to submit is passport, which would then be photographed by PXXX. Coerced consent is no consent at all.

This serves as sufficient basis for the Commission to waive the technicalities cited by Respondents in the absence of a Special Power of Attorney or Secretary's Certificate, which they claim to be their basis for not entertaining the letters.

*Respondent did not obtain valid consent from Complainant to collect and process personal and sensitive*

[47] PNB v. Court of Appeals, G.R. No. 218901, 15 February 2017.

*personal information from their members*

The Complaint pertains to Respondent Corporation's requirement that Complainant's church members submit their original passports, valid government IDs bearing their residence addresses in the Philippines, and colored ID pictures. The employees of Respondent Corporation then took photos of the church members' passports and valid IDs using their personal mobile phones.[48] The employees used those identification documents to produce another ID to be paid for by Complainant's church members.[49] The IDs issued by Respondent Corporation, with the bearers' addresses prominently displayed in front,[50] would have to be used by the church members in entering the building.[51]

The passports and government-issued IDs of the Complainant's church members contain both personal information and sensitive personal information as defined under the Data Privacy Act.[52]

Under the Data Privacy Act, the processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

> (a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
>
> (b) The processing of the same is provided for by existing laws and regulations: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
>
> (c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

[48] *Supra* note 1, at 61.
[49] *Id.*, at 5.
[50] *Id.*, at 145.
[51] *Id.*, at 42 dated 26 May 2019.
[52] Data Privacy Act, §3.

> (d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: Provided, That such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, That the sensitive personal information are not transferred to third parties: Provided, finally, That consent of the data subject was obtained prior to processing;
>
> (e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or
>
> (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."[53]

Respondents anchor the processing of such information on the supposed consent given by Complainant's church members, through its church elders, and on the legitimate interest of maintaining security inside the building.

In both their Responsive Comment[54] and Addendum to the Motion for Reconsideration,[55] Respondents relied on the e-mail dated 25 June 2019 from one of Complainant's church elders, PMH, to show that consent was given to allow them to process the information of all the church members:

> To: RCM
> OIC-Admin. Dept
>
> Cc: AD
>
> Re: Our MNLC willing to use your I.D.
>
> Dear Gentlemen,
>
> We are willing to use the I.D. cards that are provided by you. We request you to increase the number of manpower on Sunday to facilitate smoother distribution of ID cards as large number of people gather at the same time.

[53] *Id.*, §13.
[54] *Supra* note 1, at 341.
[55] *Id.*, at 294-295

> Our Church will cover the extra cost of the reinforcement of manpower on Sunday (June 30th).
>
> And, we would like to request you to set up separate table for those people who were not able to scan I.D. because they could not attend the worship service three weeks ago.
>
> We hope to continue maintenance good relationship your PXXX Corp.
>
> Thanks and very truly your's
>
> Mr. PMH
> Head, Admin of MNC[56]

Further, Respondents cited another email dated 26 June 2019 from IKP to Respondent RCM. They claimed that this email is the affirmation of Complainant's willingness to use Respondent Corporation-issued IDs. The said e-mail states:

> Hi RCM!
>
> This is Elder IKP of MNLC and Good morning !
>
> Regarding MXXX ID,
>
> Our MNLC's Chief Administration Officer PMH already submitted yesterday our letter to confirm to use MXXX ID from coming Sunday (June/30~~~ )
>
> And happy to solve this hectic pending issue each other under the love of same God and Jesus Christ.[57]

The Data Privacy Act provides that the consent of a data subject must be a "freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her… It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so."[58] The Data Privacy Act also requires that "[c]onsent shall be evidenced by written, electronic or recorded means."[59]

---

[56] *Id.*, at. 341 and 348.
[57] *Id.*, at 340 and 347.
[58] Data Privacy Act, §3(b).
[59] *Id.*

In determining whether consent was freely given, the data subject must be given a real choice where there is no risk of deception, intimidation, coercion or significant negative consequences if he or she does not consent. If the consequences of giving consent undermine the individual's freedom of choice, consent would not be free.[60] For instance, a "bundled" consent will generally not suffice as the data subject is not empowered to make a true choice.[61]

The e-mails quoted in both the Responsive Comment[62] and Addendum to the Motion for Reconsideration[63] of Respondents, supposedly an indication of consent as a lawful basis for processing, must be contextualized. It must be noted that said e-mails were sent after several events have already transpired involving Complainants' church members and Respondents. Two (2) respected church members were banned from entering the premises and exercising their religion, an event that frightened most of the church members.[64] Guard dogs were posted at the entrance of the building. Churchgoers were delayed for over an hour and a half before they can enter the building leaving most seats still vacant by the time their worship started.[65] These allegations in the Complaint-Affidavit remain to be unrefuted by Respondents, thus:

> On 12 May 2019, tempers flared resulting in exchange of words between MNLCI members and PXXX's guards. In a letter dated 15 May 2019, PXXX banned two (2) respected church members, MH and LSB, from entering the Building from 14 to 19 May 2019.
>
> Guard dogs are posted at the entrance and churchgoers are delayed for as long as an hour and a half before they can enter the Building. They attach pictures of the long line at the entrance endured by MNLCI's members on 23 June 2019, thereby leaving mostly vacant seats by 11:00AM, which is the start of our time of worship during Sundays. Such form of harassment was implemented by PXXX by significantly reducing the entrance line to one, intended to force churchgoers to surrender their passports and valid ID's for

[60] National Privacy Commission. Advisory Opinion 2019-034 Re: Consent and Its Withdrawal for Employment Purposes. 02 September 2019, *citing* European Commission, Article 29, Data Protection Working Party, Opinion 15/2011.
[61] National Privacy Commission. Advisory Opinion No. 2018-013 Re: Privacy Policy and Consent of Data Subjects. 18 April 2018.
[62] *Supra* note 1, at 341.
[63] *Id.*, at 294-295.
[64] *Id.*, at 73.
[65] *Id.*, at 3.

> processing by PXXX's employees, supposedly for the production of PXXX-issued ID's that shall be paid for by MNLCI's members.[66]

Clearly, the supposed consent of Complainant's church members relied upon by Respondents cannot be considered freely given as required by the Data Privacy Act. An imbalance already exists between the controller and the data subject. Respondents not only controlled the MNLC members' access to their place of worship, which they describe as the "really most important and worthy matter in their whole life,"[67] but they have already demonstrated their willingness to assert this control by banning church members and posting guard dogs.

Taking all the circumstances of this case into consideration, it can be seen that the e-mails from church elders of complainants relied upon by Respondents were written in light of the growing tension between Respondents or the personal information controller on the one hand, and Complainant's church members or the data subjects on the other. In fact, in the email of IKP dated 28 June 2019, cited by Respondents in their Motion for Reconsideration, he categorically stated that their use of the MXXX ID was purely for the purpose of smooth and quick entrance process for normal and spiritual worship, especially for the church members who did not submit yet their copies of Government IDs.[68] From this it can be seen that the supposed consent was given only so that the church members can attend worship services peacefully. Given all the pressure exerted on them, including being forced to choose between giving up their privacy or the exercise of their religion, it cannot be said that the church members were empowered to make a true and free choice.[69] Clearly, this kind of consent is invalid.

This Commission also notes that Complainant, in its letter to Respondents dated 04 June 2019, already categorically stated that the latter's act in collecting passports, residential data, and photographs from Complainant's church members was not voluntary and that while some of their members may have submitted these documents it was just for the purpose of gaining access to their place of worship.[70] This not only reinforces the fact

---

[66] *Id.*, at 3 to 5.
[67] *Supra* note 2, at p. 10.
[68] *Supra* note 1, at 343 and 350.
[69] National Privacy Commission. NPC Advisory Opinion 2018-063 Re: Review of Consent Form. 23 October 2018.
[70] *Supra* note 1, at 44.

that no consent was validly given by Complainant's church members, but more importantly, Respondents were aware of such fact.

This awareness is borne out in the cross-examination of Respondent AD where he admitted that no written consent was obtained from Complainant's church members prior, during or after the processing of their personal data. Clearly, the supposed consent relied upon by Respondents is entirely based on the emails of some Complainant's members and not the written, electronic, or recorded consent of the individual church members as required by the Data Privacy Act.

Given all these, Respondents processed the personal data of the Complainant's church members without the consent of the data subjects as defined under the Data Privacy Act.

This Commission also notes the inconsistent manner in which Respondents deal with MNLCI and its representatives – questioning the authority of Complainant's representatives to file this case for the entire congregation while relying on practically the same representatives and claiming that they consented for everyone else. Respondents cannot have it both ways.

*Respondent cannot rely on legitimate interest to collect and process personal and sensitive personal information from Complainant's members*

Previously, Respondent Corporation only required that the church members of the Complainant wear insignias or stickers during Sundays.[71] Thereafter, Respondents required the Complainant to produce IDs for their church members to be used in entering the building every Sunday.[72] Witnesses for Complainant testified that MNLCI produced IDs for their church members for their worship

[71] *Id.*, at 29.
[72] *Id.*, at 30.

days within the building.[73] Respondent AD admitted this fact in his 16 May 2019 letter to Complainants where he said:

> [W]e appreciate that the MNLC, thorugh the indomitable will and persistence of PMH, have at long last abided by the requirement of providing ID's to the members of MNLC, however after much review of your Identification Cards, our security and safety consultants have observed that the archetype of MNLC Identification Cards are without a doubt susceptible to security breach, which may include but not limited to, meagre (sic) identification control system and counterfeit.[74]

During the summary hearings, however, Respondent AD, while acknowledging that Complainant already provided IDs to its members, gave a different reason why Respondents rejected these IDs. He explained that while the MNLC-issued IDs showed both the Korean and English names of the church members, the Korean characters were bigger and more prominent. He stated that this was a security threat to the other tenants of the building, because only the church members can read and understand the Korean characters.

Despite their compliance with Respondents' requirements of producing the IDs for its church members, for the reasons stated above these were disallowed and Complainant's church members were required to submit their passports and valid IDs bearing their Philippine residence address in order to enter the building for their Sunday worship. [75] Respondents' employees took photos of the passport and IDs of Complainant's church members using their personal mobile phones and used the gathered personal data to produce and issue its own ID for which it charged a fee.

Respondents justified the processing of these personal data supposedly for purposes of their legitimate interest to enforce building security rules and regulations in light of the reported recent incidents. The relevant portions of the Respondents' buildings and regulations with regard to the "No ID, No Entry" policy provide:

> 3.4 Office visitors and clients maybe allowed entry when properly identified and acknowledged by person/s to be visited and prior

[73] *Id.*, at 76.
[74] *Id.*, at 34.
[75] *Id.*, at 136.

> processing by building security. Person/s not properly identified or owned by an authorization from unit owners or tenants shall not be allowed entry beyond regular hours.
>
> Office visitors and clients must present and deposit a valid Identification Card with their picture, in exchange for a visitor's card. Valid IDs shall be current issues of the following:
>
> 3.4.1 Passport
>
> 3.4.2 Driver's license
>
> 3.4.3 PRC ID
>
> 3.4.5 Voter's ID, TIN, SSS
>
> 3.5 Visitors shall complete the registration form with information regarding their visit and shall be provided a building pass for security purposes. It is understood that PXXX Corp. protects the data and information collected through the registration form using technical, physical and administrative security measures to reduce the risk of loss, misuse, unauthorized access, disclosure or modification of the given information and will only retain the information collected as long as it is reasonably needed for each purpose.[76]

Despite Complainant's compliance in producing the IDs for its church members and the clarifications sought from Respondent to produce its own IDs, Complainant was unable to prevent the copying of their church members' identification documents and the production of IDs displaying their Philippine residence.[77] These were suddenly required in order to enter the building for their Sunday worship. In disallowing the use of Complainant-issued IDs, Respondents decided to provide IDs for a fee after gathering the identification documents from Complainant's church members.

Respondents argued that these strengthened security measures are necessary to protect the safety, health, and life of the church members following several incidents of breaking and entering, theft, vandalism, and other occurrences that causes fright to the tenants.[78]

---

[76] *Id.*, at 190 and 191.
[77] *Id.*, at 136.
[78] *Id.*, at 343.

While the security of the premises and tenants of the building is a legitimate interest, the fact remains that these stricter security measures are only applied to Complainant's church members and not to the other tenants of the building.

There is nothing on record that would remotely show that the church members were suspected to be behind any of the security incidents mentioned by Respondents. In one incident report, a church member of the Complainant was even the one who witnessed a certain individual posting decals on the building premises.[79] In another incident where fire hose nozzles were stolen, a non-resident was identified as a suspect.[80]

*Respondent did not observe the principle of proportionality in collecting and processing personal and sensitive personal information from Complainant's members*

Respondents insisted that the collection and processing of Complainant's church members personal data from passports and government-issued IDs is proportional to their legitimate interest to ensure safety and order within the premises of the building.[81] However, the principle of proportionality requires that the processing of personal information must be relevant to, and must not exceed, the declared purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.[82] Hence, proportionality is met when the processing is the least intrusive measure to achieve its purported aims.[83]

---

[79] *Id.*, at 219-220.
[80] *Id.*, at 239-240.
[81] *Id.*, at 344.
[82] Implementing Rules and Regulations (IRR) of R.A. 10173. §18(c).
[83] ICCPR, Art. 19; General Comment 34, par. 34; UNHRC, 'General Comment No. 22: Article 18 (Freedom of Thought, Conscience or Religion), (30 July 1993) UN Doc CCPR/c/21/Rev.1/Add.4 ('General Comment 22'), par. 8; Shelton v. Tucker, 364 US 479

In this case, the requirement of submission of passports, government-issued IDs, and colored ID pictures is not the least intrusive means to achieve the desired purpose. The IDs issued by Complainant to its church members should suffice as an exhibit of the authorization as required under the building rules.[84]

This fact was recognized by Respondents when they alleged in both their Motion for Reconsideration[85] and Responsive Comment[86] that they have been constantly reminding Complainant to provide even just an emblem, insignia or even as simple as stickers, where security guards on duty can positively identify their church members. They claim, however, that the security measures they implemented as against Complainant and its members were justified "because of MNLC's delay and unjustified refusal."[87]

Respondents seem to have forgotten their previous statements and admissions in making this claim. As discussed above, Respondent AD acknowledged in his 16 May 2019 letter and during the summary hearing that Complainants already issued ID cards to its members. In both those instances, Respondent AD gave inconsistent reasons why Respondents disallowed the ID cards issued by Complainants: susceptible to security breach on the one hand, and the Korean names were bigger and prominently than the English names on the other. Apparently, Respondents' claim that all they are asking Complainant to provide is "just an emblem, insignia or even as simple as stickers so that the security guards on duty can identify their church members,"[88] is clearly not true.

Setting aside for a moment the validity and veracity of those reasons, including whether Respondents have the necessary security measures and systems in place such that their own issued IDs are not susceptible to the same security issues they claim in relation to the IDs issued by Complainant, their previous assertions belie Respondents' current claim on the necessity and proportionality of the measures it adopted.

---

(1960); Thorgeirson v. Iceland App No. 13778/88 (ECTHR, 25 June 1992).

[84] *Supra* note 1, at 190 and 191.

[85] *Id.*, at 291.

[86] *Id.*, at 344.

[87] *Ibid.*

[88] *Ibid.*

The fact that none of Respondents' alleged reasons for disallowing the IDs Complainant issued to its members find basis in any of its documented policies also argues against the proportionality of these measures. As this Commission noted in its Resolution denying Respondents' Motion for Reconsideration:

> In determining what information can be collected for and displayed on the ID card, the respondents must consider the purpose for such ID. The above-cited House Rules and Regulations signifies that the ID is an exhibit of such authorization to enter from the building tenant. There is no documented policy which declares that the ID card should serve other purposes, nor is there anything that requires the tenant to be supported by 201 file records or to have specific security measures.[89]

The availability of a far less intrusive measure demonstrates that the measures employed by Respondents are disproportionate to the aim they seek to achieve. Inasmuch as Respondents recognized the issued IDs of the other tenants in the building, the same standard should have been applied to the church members of Complainant. The subject measure cannot be considered proportionate to the claim of increased security in the premises of MXXX Building.

This is all the more true considering Respondent AD's letter to the Bureau of Immigration (BI) and copy-furnishing the Embassy of the Republic of Korea, the Department of Foreign Affairs, and the Mayor of the City of Makati, dated 24 June 2019. The letter stated thus:

> [W]e ardently request your office to look into this matter as there might be Korean Nationals members of the MNLC who have expired VISA or undesirable aliens or fugitives from other countries.
>
> xxx
>
> Thank you very much and in the highest interest of justice and peace, we fervently seek your office's intervention on the

[89] *Id.*, at. 374-375.

> legality and validity of the immigration and alien admission of the members, pastors and elders of the MNLC.[90]

By no stretch of reasoning can the involvement of the BI be considered as necessary to fulfill the declared purpose of security measures in the building. The request for the BI's intervention in investigating the validity of the Korean nationals' visas only strengthens the conclusion that the application of strict security measures were specifically targeted to the Complainants' members and hence excessive to the declared purpose of building security measures.

The previous Order[91] of this Commission granting the request for Temporary Ban discussed this matter, thus:

> PXXX cites security measures as the declared purpose for requiring the validation of passports and government-issued IDs of MNLCI's church members. However, **the fact that the stricter security measures applied only to MNLCI's church members, and not the other tenants of the building, cannot be justified as proportional.** The recognition of validly-issued MNLCI IDs should be considered as sufficient to meet the authorization requirements for entrance to the building, in as much as PXXX recognizes the company-issued IDs of its other tenants. The negative effects that these security measures have caused cannot be overlooked.[92]

*The Compliance ad Cautelam is not sufficient*

At the outset, the Commission wishes to clarify a misconception by the Respondent Corporation with regard to the public's compliance to the Orders issued by the Commission. In their Counter-Manifestation dated 03 October 2019, they state:

> 6. [C]onsidering that the filing of a motion for reconsideration is regarded as part of "due process of law" respondents cannot be barred from filing the same. To proceed with the implementation of the Order dated 11 September 2019 notwithstanding the timely filing of the motion for reconsideration would be tantamount to disregarding respondent's right to due process of

[90] *Id.*, at 62-63.
[91] Order dated 11 September 2019.
[92] Emphasis supplied.

> law as it would render naught the latter's right to question the propriety of the assailed order of this Honorable Commission.[93]

Aside from the lack of support in law or in regulations, Respondents failed to consider that the NPC Rules of Procedure clearly indicate the period of effectivity of a Temporary Ban on Processing Personal Data, thus:

> SECTION 19. Temporary Ban on Processing Personal Data – At the commencement of the complaint or at any time before the decision of the National Privacy Commission becomes final, a complainant or any proper party may have the National Privacy Commission, acting through the investigating officer, impose a temporary ban on the processing of personal data, if on the basis of the evidence on record, such ban is necessary in order to preserve the rights of the complainant or to protect national security or public interest…
>
> xxx
>
> d. **If so issued, the temporary ban on processing personal data shall remain in effect** until the final resolution of the case or upon lawful orders of the Commission or lawful authority.[94]

In the Respondents' eventual submission of its Compliance *Ad Cautelam*, the Commission notes that other than bare allegations, Respondents failed to provide proof that they no longer require the Complainant's members to use PXXX-issued IDs. Notably, two (2) months after the Commission's denial of the Motion for Reconsideration of the Respondents, Complainants filed a Manifestation that Respondents still refused to allow Complainant's members to enter with MNLCI-issued IDs.[95]

In an e-mail to the Commission on 06 November 2020, Mr. GSP, a member and deacon of MNLCI, detailed the security measures implemented by PXXX in relation to Complainant's members:

> NPC has requested to confirm, if the Peaceland (sic) (Building owner; "PL") do not require PL issued ID for entrance?

---

[93] *Supra* note 1 at 327-329.
[94] Section 19, NPC Circular No. 16-04. Rules of Procedure of the National Privacy Commission. Dated 15 December 2016. Emphasis supplied.
[95] Manifestation and Motion by Complainant, dated 3 February 2020.

> 1. Officially, PL do not make it *(sic)* a requirement to present PL ID.
>
> PL, however, before lock-down, have allowed those with PL ID to enter without difficulties.
>
> Those without PL ID, had to (1) quey (*sic*) up in long lines, (2) present PH gov't issued ID (any other ID denied), (3) register all names of family, just to enter for worship services.
>
> This practically made it impossible for those who have no PH gov't ID at hand.
>
> More important, PL did not apply such strict restrictions to those of other tenants on other floors, as they simply entered with their own tenant IDs.
>
> With no grounds, PL did not allow MNLCI ID. It is even more unjust, as MNLCI is owner of our two floors, and we are not even tenants.[96]

While the Respondent Corporation no longer officially requires the Complainant's members to use their building ID, the Commission finds that their practices of requiring additional documents and information only from Complainant's members and not its other tenants effectively continue to defy the Order of the Commission dated 11 September 2019[97] which: 1) imposed a temporary ban on the processing of the personal data of Complainant's church members who have not yet provided their identification documents to Respondents, and 2) required Respondent to allow Complainant to provide IDs for their church members and officers bearing only their photos and English names.

*Respondents are liable for unauthorized processing of personal and sensitive personal information of Complainant's members*

[96] Email dated 6 November 2020 by GSP.
[97] *Supra* note 21.

In determining whether a violation of Section 25(b) of the Data Privacy Act 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.[98]

As to the first element, the Data Privacy Act 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."[99] Simply stated, processing refers to any use of personal data at any stage of the data life cycle.

In this case, it has been established that Respondents processed the information of Complainant's members through the required collection of original passports, valid IDs bearing their Philippine residence addresses, and colored ID pictures, which were later on stored.

As to the second element, the information subject of this case is sensitive personal information. Under the Data Privacy Act, 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;

[98] NPC Case No. 17-018, Decision dated 15 July 2019.
[99] Data Privacy Act, §3(j).

> 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.[100]

Considering the collection of government IDs and passports, the exposure of the Complaint's members race, ethnic origin, age, and government-issued identifiers is inevitable.

With regard to the third element, the Commission has extensively discussed that the Respondents failed to present any valid criteria for the lawful processing of the church members' personal data. The Commission has also found an inability by Respondent to show adherence with the data privacy principles of transparency, legitimacy, and proportionality.

Following this, the Commission finds that Respondents' processing of the personal information of the Complainant's members meets all the elements of Section 25(b) of the Data Privacy Act.

Considering that Respondent PXXX is a Corporation, Section 34 of the Data Privacy Act applies, thus:

> Section 34. Extent of Liability. If the offender is a corporation, partnership, or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime.

The Commission notes the direct involvement of Respondent AD, as the Head of the Legal & Corporate External Affairs Deparment, and Respondent RCM, as the Office in Charge of the Administration Department, in the Respondent Corporation's collection of sensitive personal information from Complainant's members. The Commission also notes the communications made by Complainant's counsel to the Respondents' Board of Directors

[100] *Id.,* at § 3(l). Emphasis supplied.

that repeatedly raised this concern. Despite being apprised of the issues, the Board of Directors nevertheless allowed such unauthorized practices to persist.

In addition, the actions of Respondents in continuing to process the information of Complainant's church members in a manner inconsistent with how it treats its other tenants in defiance of this Commission's Order demonstrates not just gross negligence but bad faith on their part.

*Complainant's members are entitled to damages*

The Data Privacy Act provides that every data subject has the right to be indemnified for "any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information."[101] Indeed, it is part of the Commission's mandate to award indemnity on matters affecting any personal information.[102]

It is worth noting that the Data Privacy Act does not require actual or monetary damages for data subjects to exercise the right to damages. As provided in the law, the consequences of processing inaccurate information is enough for the right to arise.[103]

The Data Privacy Act provides that restitution for any aggrieved party shall be governed by the provisions of the New Civil Code.[104] The relevant provision in this Code states:

> Art. 2221. Nominal damages are adjudicated in order that a right of the plaintiff, which has been violated or invaded by the defendant, may be vindicated or recognized, and not for the purpose of indemnifying the plaintiff for any loss suffered by him.

[101] *Id, at* §16(f).
[102] *Id.,* at §7(b).
[103] *Ibid*.
[104] *Id.*, §37.

The Data Privacy Act gives individuals the right to receive indemnification from personal information controllers and personal information processors for both material and non-material damages.[105] The Supreme Court has also clarified that no actual present loss is required to warrant the award of nominal damages, thus:

> Nominal damages are recoverable where a legal right is technically violated and must be vindicated against an invasion that has produced no actual present loss of any kind or where there has been a breach of contract and no substantial injury or actual damages whatsoever have been or can be shown.[106]

Pursuant to the New Civil Code and following the aforementioned findings that Respondents not only unlawfully processed the subject sensitive personal information but also failed to observe the general privacy principle of proportionality, the Commission finds that the award of nominal damages to Complainant is warranted.

**WHEREFORE**, all premises considered, this Commission hereby:

1. **FINDS** that Respondent AD, Respondent RCM, and the Board of Directors of PXXX Corporation, namely EPA, CAS, RCM, HAB, and JRB, as its responsible officers, have violated Section 25(b) of the Data Privacy Act;

2. **FORWARDS** this Decision and a copy of the pertinent case records to the Secretary of Justice, recommending the prosecution of respondents for the crime of Unauthorized Processing under Section 25 of the Data Privacy Act, and for its further actions;

3. **AWARDS** damages, in the amount of P1,000.00, to each member of Complainant MNLC as of the date of filing of the Complaint Affidavit on 23 July 2019 for Respondent's

[105] *See,* Handbook on European Data Protection Law, p. 246.
[106] Seven Brothers Shipping Corporation v. DMC-Construction Resources, Inc. G.R. No. 193914. November 26 2014.

unlawful collection of their sensitive personal information, pursuant to Section 16 (f) of the Data Privacy Act; and

4. **ORDERS** the submission of proof of compliance by Respondents' with abovementioned award within thirty (30) days of receipt of this Decision.

**SO ORDERED.**
Pasay City, Philippines;

29 October 2020.

**Sgd.**
**LEANDRO ANGELO Y. AGUIRRE**
*Deputy Privacy Commissioner*

WE CONCUR:

**Sgd.**
**RAYMUND ENRIQUEZ LIBORO**
*Privacy Commissioner*

**Sgd.**
**JOHN HENRY D. NAGA**
*Deputy Privacy Commissioner*

**COPY FURNISHED:**

**AAC LAW OFFICES**
Counsel for the Complainant

**MP LAW OFFICE**
Counsel for the Respondents

**ENFORCEMENT DIVISION**
**GENERAL RECORDS UNIT**
National Privacy Commission