Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2023-010[1]

15 February 2023

[redacted]

RE: RECORDING OF TELEPHONE CONVERSATION THROUGH VOICE OVER INTERNET PROTOCOL (VoIP) SYSTEM

Dear [redacted],

We respond to your query about the conversation recording feature of the Voice Over Internet Protocol (VoIP) telephone system of the Philippine Merchant Marine Academy (Academy).

You explained in your letter that the VoIP phone is a hardware or software-based telephone that is designed to use VoIP technology to send and receive calls over an IP network. Through this technology, calls can be recorded entirely in the cloud or on-premises with VoIP call recording software. You mentioned that the system automatically records and saves outgoing telephone calls. The system is being managed by your Information Technology Services Unit (ITSU) which released a policy on the use of VoIP phones, as follows:

> Personnel shall not use the Services for any illegal, fraudulent, improper, or abusive purpose.
>
> 1. Use PMMA Phones for business purposes only and preserve them in perfect condition.
> 2. The international call is available for an additional fee.
> 3. Except in the case of employees provided with private telephone lines, all outgoing telephone calls shall course through the Information Operator.
> 4. The telephone operator shall be obliged to maintain the telephone logbook and submit it to the respective authority at the end of the month."

[1] Tags: lawful processing; legitimate interest; proportionality; security measures.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph * Tel No. 8234-2228

You also mentioned that the Academy's Data Privacy Office and ITSU are currently revisiting the policies on the usage of VoIP phones since the current policy does not include conversation recording. Neither have the employees been notified of this recent feature.

You thus ask whether the automatic conversation recording feature of the VoIP phone can lead to a possible violation of the DPA and other laws or regulations.

Scope of the Data Privacy Act; lawful processing; recorded calls containing personal data; proportionality.

RA 10173 or the Data Privacy Act of 2012 (DPA) applies to the processing of all types of personal information [2] and to any natural and juridical person involved in personal information processing.[3]

Processing as defined under the DPA refers to 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.[4]

Recording telephone conversations may be considered as a form of data processing since personal information and sensitive personal information (collectively, personal data) may be given out or spoken in the course of these conversations. In NPC Advisory Opinion No. 2017-63[5], the concept of biometrics as personal data was discussed, *viz.*:

> "Under Republic Act (RA) No. 10367 [6], biometrics refer to 'the quantitative analysis that provides a positive identification of an individual such as voice, photograph, fingerprint, signature, iris and/or such other identifiable features.'[7]
>
> While under Article 29 Opinion 4/2007 (EU)[8], a biometric data may be considered both as content of the information about a particular individual as well as an element to establish a link between one piece of information and the individual. As such, it can work as "identifier" for it produces a unique link to a specific individual.
>
> On that note, it must be emphasized that DPA defines personal information as "any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual." [9] Corollary, hand-

[2] Data Privacy Act of 2012, § 3 (g). *Personal information* refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.
[3] *Id.* § 4.
[4] Data Privacy Act of 2012, § 3 (f).
[5] National Privacy Commission, NPC Advisory Opinion No.2017-063, (09 February 2017).
[6] AN ACT PROVIDING FOR MANDATORY BIOMETRICS VOTER REGISTRATION, 15 February 2013, §2(b).
[7] R.A. No. 10367, §2(a).
[8] Opinion 4/2007 on the concept of personal data, Adopted on 20th June 2007.
[9] Id., § 3(g).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph * Tel No. 8234-2228

written signatures, as may be used to identify an individual, is considered as personal information.

In the same manner, unique information relating[10] to an individual or when linked with other information will allow an individual to be distinguished from others, may be treated as personal information." (underscoring supplied)

In your query, the recording of a telephone conversation is considered as processing of personal data when the parties to the conversation can be identified by their voice; or when linked to other information can identify an individual/s, such as an employee directory, or if the caller's identity is mentioned in the phone conversation.

The processing of a telephone conversation *via* recording is not prohibited by the DPA, but there must be a legitimate purpose for recording and such purpose is not contrary to law, morals or public policy. If a legitimate purpose has been established, the next step is to determine the applicable criteria for processing under Section 12 or 13 of the DPA, depending on the personal data involved, thus:

> **SEC. 12. Criteria for Lawful Processing of Personal Information. –** The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:
>
> (a) The data subject has given his or her consent;
>
> (b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
>
> (c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
>
> (d) The processing is necessary to protect vitally important interests of the data subject, including life and health;
>
> (e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
>
> (f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

[10] EU Directive 95/46/EC Working Party Document No. WP 105 noted that "Data relates to an individual if it refers to the identity, characteristics or behavior of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated."

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph * Tel No. 8234-2228

> **SEC. 13. Sensitive Personal Information and Privileged Information. –** 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;
> >
> > (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.[11]

In your letter, the following are the stated purposes for the automatic recording of the Academy's outgoing calls through the VoIP system,:

> 1. to keep detailed call records;
> 2. to recover missed details; and
> 3. to protect the Academy and its employees and any possible *potential* legal dispute and for security reasons.

Based on the aforementioned purposes, it appears that the only applicable basis for processing would be to obtain the consent of the data subjects.

As presented, the purposes seem to be ambiguous and speculative; hence, they cannot qualify under the criterion of legitimate interest in Section 12 (f) of the DPA. The purposes failed to state what specific details would be recorded or are sought to be recorded to justify the

[11] *Id.* § 12,13.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph * Tel No. 8234-2228

automatic recording. This contravenes the data privacy principle of transparency which requires that the data subject (i.e., the parties to the telephone conversation) must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised.[12]

The automatic recording of VoIP phone calls also appears to be disproportionate to the purposes it seeks to achieve. The data privacy principle of proportionality requires that 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.[13] The Academy has not shown that the purposes stated in the VoIP policy cannot be fulfilled through any other means aside from the recording of the phone calls.

Lastly, the enumerated purposes appear to be speculative and have no specific legal basis to rationalize the recording of conversations without the consent of the parties to the phone call.

Reasonable expectation of privacy in the workplace

Factual circumstances of every case determine the reasonableness of the expectation of privacy. Similarly, customs, community norms, and practices may, therefore, limit or extend an individual's reasonable expectation of privacy. The reasonableness of a person's expectation of privacy is determined on a case-to-case basis.[14]

NPC Advisory Opinion No. 2018-090[15] is highly instructive on the reasonable expectation of privacy in the workplace in light of the implementation of the DPA, *viz.*:

> Likewise, courts have generally held that employees have a decreased expectation of privacy with respect to work devise, email accounts, and internet surfing activities. The same may be said for the contents therein, since there is an assumption that its use will be limited to work-related purposes.
>
> Yet, with the DPA now in place, the reasonable expectation test should be revisited and interpreted in the context of the law.
>
> By virtue of a legislation on data protection and privacy, the assumption is that individuals now have an expectation of privacy. As to the second element, data privacy is now more than a reasonable expectation – it is now enshrined in the DPA. The reasonable expectation of privacy test then should take into consideration the standards provided under the DPA.
>
> This means that employees must be aware of the nature, purpose, and extent of the processing of his or her personal data in the workplace. The processing of personal information of employees shall also be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. Lastly, the processing of such information shall

[12] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18(a) (2016).
[13] *Id* § 18(c) (2016).
[14] National Privacy Commission, NPC Advisory Opinion No. 2018-090 (28 November 2018).
[15] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph * Tel No. 8234-2228

> be adequate, relevant, suitable, necessary and not excessive in relation to a declared and specified purpose.

Recent jurisprudence from foreign jurisdictions also provide guidance with regard to monitoring calls of employees at the workplace. In *Copland v. the United Kingdom,*[16] the European Court of Human Rights (ECtHR) held that monitoring calls without the employee's knowledge, amounted to unnecessary interference with his privacy rights, *viz:*

> 42. The applicant in the present case had been given no warning that her calls would be liable to monitoring, therefore she had a reasonable expectation as to the privacy of calls made from her work telephone (see Halford, § 45). The same expectation should apply in relation to the applicant's e-mail and Internet usage.
>
> xxx
>
> 44. Accordingly, the Court considers that the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and Internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence xxx.
>
> xxx
>
> 47. The Court is not convinced by the Government's submission that the College was authorized under its statutory powers to do "anything necessary or expedient" for the purposes of providing higher and further education, and finds the argument unpersuasive. Moreover, the Government do not seek to argue that any provisions existed at the relevant time, either in general domestic law or in the governing instruments of the College, regulating the circumstances in which employers could monitor the use of telephone, e-mail and the Internet by employees.

Hence, with the DPA in place, employers are expected to be more mindful of the privacy rights of their employees.

Privacy notice; privacy policy; data security

In your letter, you mentioned that no notice has been disseminated yet on the automatic recording feature of the VoIP phone. We recommend that the Academy gather the consent of the data subjects which may be done through an automatic voice prompt informing the data subjects that the conversation will be recorded for the purposes cited in your VoIP policy. This is also a good way to notify the data subjects of the nature, purpose and extent of the processing of their personal data.

Further, please note that the upgrade in the system necessarily signifies the need to revisit the Academy's security policies. We suggest the drafting a more comprehensive privacy policy which would also include other provisions on data privacy such as data retention, deletion, and access.

[16] ECtHR, Copland v. the United Kingdom, No. 62617/00, 3 April 2007

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https://www.privacy.gov.ph Email Add: info@privacy.gov.ph * Tel No. 8234-2228

Moreover, a Privacy Impact Assessment (PIA) may be necessary prior to the introduction of this telephone system to identify existing and potential risks and enable the Academy to take the appropriate measures. A PIA will help you identify the type of security demanded on this kind of medium for personal data. A PIA will ensure the system's compliance with the DPA and protection of your data subject's rights:

> A PIA should be conducted prior to the deployment of a project, product, or service that involves the collection of personal information. When there are new or revised industry standards, organization policy, law or regulation, or when there are changes to methods in which personal information is handled, a personal information controller should conduct a PIA again on the pertinent process.
>
> To emphasize, it should not only identify the existing controls and risks a project, product, or service may have upon personal data privacy, but it should lead to the identification of remedial actions or mitigation measures necessary to avoid or reduce those risks. These remedial actions and mitigation measures may be incorporated in the organization's Privacy Management Program (PMP).[17]

As to your query on the other possible legal repercussions of the Academy's adoption of the system, (e.g. the Anti Wiretapping Law), it would be best to consult your legal department as they possess all the necessary information and facts to respond appropriately.

Please be advised that the foregoing was rendered based solely on the information provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Note that this communication is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

[17] KRL vs. Trinity University of Asia, AA, MC, NCB, RG GV, GCT, RR, MR, PB, CID Case No. 17-K-003 (19 November 2019).