University of the Philippines Diliman
Data Protection Team

upd.edu.ph/privacy
dpo.updiliman@up.edu.ph
(632) 8255-3561

10 October 2019

ADVISORY OPINION

Reference No. DPO 19-44

FOR : [redacted]

[redacted]

[redacted]

CC: [redacted]

SUBJECT : **Data Protection Measures for Implementation of RFID System**

Dear [redacted], [redacted], and [redacted]:

We respectfully provide guidance on ensuring data privacy in the implementation of the RFID System.

Facts

- The University is adopting the use of the use of Radio Frequency Identification (RFID) cards to all students, faculty and staff through a non-exclusive partnership with [redacted] ("[redacted]").
- Holders of the RFID may avail of "additional features and services".
- Office of the President Memorandum No. PDLC-19-14 ***directed*** UP Diliman to implement the RFID System for all its eligible constituents effective the First (1st) Semester of Academic Year 2019-2020.
- On 18 September 2019, a consultation meeting was held among representatives of [redacted], [redacted], [redacted] and [redacted] to prepare for the implementation of the RFID System.

- On 02 October 2019, the UPD [redacted] received a letter from the [redacted] requesting that assistance to [redacted] and [redacted] be provided in the operationalization of the RFID System in UP Diliman.

Issues

I. What data privacy concerns, if any, should be addressed?
II. How to enforce safe transfer of data to a third party?
III. What information are required to execute a Non-Disclosure Agreement?

Advisory Opinion

I. Privacy Concerns

The RFID is a welcome initiative in terms of implementing security measures for identity verification and access management. However, since UP-issued student, faculty and staff numbers are sensitive personal information, transmitting these to a third party would require consent from the individuals involved. The concern in requesting for consent is that UP Diliman cannot impose the RFID System to those who will not grant their consent. This will force UP Diliman into a problematic situation wherein the RFID System will be selectively implemented only to those who gave their consent.

The suggested solution is to segregate the function into two processes: UP Diliman implements and RFID System and uses [redacted] as a mere subcontractor of RFID production. Separately, [redacted] opens an optional registration process for those who wish to avail of "additional features and services". This way, UP Diliman's RFID System becomes a pure government function with no consent required. [redacted] will be responsible for the data gathering and consent gathering of its separate initiative to provide "additional features and services".

Another concern is the observance of the rights of data subjects. [redacted] and [redacted] should *(i)* be familiar with the RFID's rationale and use of personal information; and *(ii)* coordinate with the DPT to be responsive to individuals invoking their privacy rights.

II. Information Security

Data at rest with UP Diliman – [redacted] and [redacted] should comply with the UP Diliman Privacy Policy and the UP Diliman Privacy Management Program Framework to maintain the confidentiality, integrity and availability of

data under the custody of their offices.

Data in transit from UP Diliman to [redacted] - The UP Diliman should be consulted on how UP Diliman can work with [redacted] to ensure that secure infrastructure and protocols are in place and are regularly tested.

Data in use by [redacted] and *data at rest with* [redacted] – The UP Diliman [redacted] conduct a vulnerability assessment of [redacted]'s data processing systems. The UP Diliman Data Protection Team should evaluate [redacted]'s compliance with the Five Pillars of Data Privacy Accountability and Compliance and establish a reporting mechanism for [redacted]'s compliance with the parties' agreement discussed below.

III. Required Agreement

The UP Diliman Data Protection Officer drafted the attached *Outsourcing, Non-Disclosure and Data Protection Agreement* which is in line with relevant privacy laws and regulations. This incorporates the necessary security measures UP Diliman should expect from [redacted] in accordance with applicable data privacy rules. This agreement contains industry-standard covenants found in Non-Disclosure Agreements and hence a separate NDA is no longer necessary.

Discussion

I. Privacy Concerns and Recommended Solutions

The University's intent to embrace technological innovations such as RFIDs for identity verification and access management is admirable. However, its implementation is not without privacy concerns.

Concern #1:

Prior consent must be obtained. If others withhold consent, it would be problematic to implement a selective RFID System which is applicable only to those who consented to the System.

The primary privacy concern is that the consents of students, faculty and staff have to be obtained prior to the use of their personal information for the RFID System.

Consent is required because the University will provide a third party UP-issued student, faculty and employee numbers which are classified as *sensitive* personal information.[1] The

[1] Data Privacy Act of 2012 Section 3(l) classifies as *sensitive* personal information those identifying information which are "Issued by government agencies peculiar to an individual". As a government instrumentality,

general rule is that sensitive personal information may not be processed unless the situation falls within the six (6) limited exceptions provided in Section 13 of the Data Privacy Act of 2012.

Sensitive personal information may not be transferred to third parties without the consent of the concerned data subjects.[2]

The RFID System's prospective utility can be dissected into the following:

First, RFIDs will be used to identify and grant access to students, faculty and staff ***("UP Diliman's Purpose")***.

Second, RFIDs may be used to optionally avail of "additional features and services" ***("[redacted]'s Purpose")***.

Since for both purposes UP Diliman will *share* sensitive personal information (*i.e.* student, faculty and employee numbers) to a third party, consents for both purposes have to be obtained.[3] Issues will arise for students that will withhold consent for one or both of the purposes. UP Diliman cannot impose the identification protocols and access requirements of the RFID System to those who will not grant their consent. From this will arise a problematic situation: having an RFID System that is selectively applicable only to those who consented to the System is a logistical conundrum if not a futile initiative.

<u>Solution #1:</u>

---

student numbers, faculty numbers and employee numbers issued by the University of the Philippines are classified as *sensitive* personal information.

[2] Data Privacy Act of 2012 Section 13 prohibits the processing of *sensitive* personal information save for limited exceptions enumerated therein. Of these exceptions, the following are relevant to the matter at hand:

> "(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;
> *x x x*
>
> (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;
> *x x x*
>
> (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**."

[3] The Data Privacy Act of 2012 Section 13 provides the circumstances where processing of *sensitive* personal information is permitted (see Footnote 2). UP Diliman may process sensitive personal information under *Section 13 (a)* as long as prior consent is obtained. Processing under *Section 13 (d)* would have been applicable if not for the transfer of information to a third party. Processing under *Section 13 (f)* would have been applicable if not for the involvement of a private organization.

Split the function into two successive steps: For *UP Diliman's Purpose*, the University can invoke that it is performing a function under government authority – hence no consent is needed. For [redacted]*'s Purpose*, a separate registration scheme can be implemented by [redacted] – hence the obligation to obtain consent will rest solely with [redacted].

The reason why prior consent is required is because UP Diliman will *share* sensitive personal information[4] to a third party. It is suggested that instead of *sharing* information for both *UP Diliman's Purpose* and [redacted]*'s Purpose*, the function is broken down into two (2) separate processes:[5]

First, for *UP Diliman's Purpose* (i.e. identifying and granting access to students), UP Diliman may *outsource* (not share) to [redacted] the process of producing RFIDs. This way, [redacted] is merely fabricating RFIDs for and on behalf of UP Diliman. At all times, UP Diliman is the controller of information[6] and [redacted] is merely an RFID vendor[7]. Through this approach, there is no *sharing* of information to a third party as contemplated by the law.[8] UP Diliman may now implement an RFID System without consent because in the absence of a third party, UP Diliman is justified to process sensitive personal information in its performance of a government authority function.[9] As additional safeguard, students were notified by the Revised UP Privacy Notice for Students[10] that their personal information will be processed for the RFID System.

Second, for [redacted]*'s Purpose* (i.e. providing "additional features and services"), [redacted] (not UP Diliman) should have a registration scheme to collect the names and UP-issued numbers directly from students, faculty and staff (with consent that [redacted] may verify their information with UP Diliman). This way, UP Diliman is separated from

[4] *Supra,* 1.

[5] "Processing" of personal information is defined by Data Privacy Act Section 3(j).

[6] Data Privacy Act Section 3(h) defines *"Personal Information Controller"* as "a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf."

[7] Data Privacy Act Section 3(i) classifies a vendor as a *"Personal Information Processor"* which is defined as "any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject."

[8] The Implementing Rules and Regulations (IRR) of the Data Privacy Act Section 43 allows the subcontracting or outsourcing of processing of personal data. This outsourcing is not considered as sharing data to a third party. It states:

> "Section 43. Subcontract of Personal Data. A personal information controller may subcontract or outsource the processing of personal data: Provided, that the personal information controller shall use contractual or other reasonable means to ensure that proper safeguards are in place, to ensure the confidentiality, integrity and availability of the personal data processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of the Act, these Rules, other applicable laws for processing of personal data, and other issuances of the Commission."

[9] Data Privacy Act Section 13 (f); see discussion on Footnote 2.

[10] Office of the President Memorandum No. TJH 2019-19.

[redacted]'s "additional features and services". At all times, [redacted] is the controller of information. Through this approach, UP Diliman will not need to obtain consent because it is [redacted] which owns the process.

Concern #2:

The Rights of Data Subjects must be observed

The Data Privacy Act of 2012 grants students, faculty and staff rights with respect to the processing of their personal information such as for the purposes of the RFID System.[11] The essence UP Diliman's compliance with privacy laws is to respect the rights of its people, including its students, faculty and staff.[12] Hence, the implementation of the RFID System should be responsive to those who will invoke their privacy rights.

Solution #2:

[redacted], [redacted] and DPT should be ready to provide invoked privacy rights.

The most fundamental and commonly invoked right is the "right to be informed" of the nature, purpose, and extent of data processing. [redacted], [redacted] and Data Protection Team (DPT) must be familiar with the new section in the Revised UP Privacy Notice for Students[13] which provides information why and how UP Diliman processes personal data for RFID purposes. When a data subject invokes the right to be informed, [redacted], [redacted] or DPT should be able to explain the RFID provisions of the Revised UP Privacy Notice for Students.

As for the other rights of data subjects, [redacted] and [redacted] are requested to coordinate with their respective Privacy Focal Persons[14] or the UP Diliman Data Protection Team in case an individual invokes a privacy right.

[11] The IRR of the Data Privacy Act Rule VIII grants the following rights to data subjects:
(1) Right to be informed of the nature, purpose and extent of processing;
(2) Right to object;
(3) Right to access;
(4) Right to data portability;
(5) Right to rectify;
(6) Right to erasure or blocking;
(7) Right to file a complaint;
(8) Right to damages; and
(9) Right to be informed of the existence of their rights.

[12] UP Diliman Data Subject Rights and Responsibilities, Office of the Chancellor Memorandum No. MLT 19-061.
[13] *Supra,* 10.
[14] Office of the Chancellor Memorandum No. MLT-18-022 establishes that UP Diliman units and offices should designate a Privacy Focal Person to uphold data protection in their respective units.

II. Information Security Requirements

Personal data must be secured[15] in all of its three (3) states[16]. The focal states in the processing of data of UP Diliman's students, faculty and staff are:

(1) *Data at rest* with UP Diliman [redacted] and [redacted];
(2) *Data in transit* from UP Diliman to [redacted];
(3) *Data in use* by [redacted];
(4) *Data at rest* with [redacted].

It should be noted that if UP Diliman pursues the solution discussed above, then UP Diliman will transmit information to [redacted] only for the purpose of outsourcing the production of RFIDs and not because it will take part in [redacted]'s "additional features and services".

Data at rest with UP Diliman – Whether to be transmitted to [redacted] or not, the data processing systems and documents of UP Diliman should have organizational, physical and technical security measures.[17] As Privacy Focal Persons of their respective offices, [redacted] of [redacted] and [redacted] of [redacted] are required by the UP Diliman Privacy Policy[18] as well as the UP Diliman Privacy Management Program Framework[19] to maintain the confidentiality, integrity and availability of data[20] under the custody of their offices.

Data in transit from UP Diliman to [redacted] – The infrastructure (hardware, software and interconnectivity) and protocols (user protocols and connection protocols) in the transfer data from UP Diliman to [redacted] should be secured. It is suggested that the UP Diliman [redacted] be consulted on how UP Diliman can work with [redacted] to ensure that secure infrastructure and protocols are in place and are regularly tested.

Data in use by [redacted] and *data at rest with* [redacted] – It is suggested that the [redacted] conduct a vulnerability assessment (and if practicable, penetration testing) of [redacted]'s data processing systems and the connectivity of these systems. The UP Diliman Data Protection Team should coordinate with [redacted]'s data protection unit to evaluate [redacted]'s compliance with the Five Pillars of Data Privacy Accountability and Compliance[21] and to establish a reporting mechanism for [redacted]'s compliance with the

---

[15] Information security ensures the confidentiality, integrity and availability of information.
Source: InfoSec Institute *(https://www.infosecinstitute.com/)*

[16] The three states of data are:
(1) Data at rest;
(2) Data in transit; and
(3) Data in use.
Sources: https://en.wikipedia.org/wiki/Data_at_rest; https://en.wikipedia.org/wiki/Data_in_transit; https://en.wikipedia.org/wiki/Data_in_use.

[17] IRR of the Data Privacy Act, Rule VI.
[18] Office of the Chancellor Memorandum No. MLT 19-061.
[19] UP Diliman Data Protection Officer Memorandum No. EBM 19-01.
[20] *Supra,* 15.
[21] National Privacy Commission Toolkit, 3rd ed., Chapter II.

parties' *Outsourcing, Non-Disclosure and Data Protection Agreement*.[22] [redacted] should not retain any personal data longer than minimally necessary to achieve [redacted]*'s Purpose*.

III. Non-Disclosure Agreement

A Non-Disclosure Agreement (NDA) is not a legal requirement but a strategic safeguard to ensure that [redacted] will not compromise the confidentiality, integrity and availability of the information processed by the RFID System. On the other hand, for *outsourcing* (not sharing) the processing of personal information to [redacted] in the production of RFIDs, the it is required by privacy rules[23] that UP Diliman (as Personal Information Controller[24]) enter into an "Outsourcing Agreement" with [redacted] (as Personal Information Processor[25]). Attached is the *Outsourcing, Non-Disclosure and Data Protection Agreement* drafted by the UP Diliman Data Protection Officer. This agreement was fashioned to incorporate above industry standard covenants commonly found in NDAs and hence a separate NDA is no longer necessary.

If UP Diliman implements the solution discussed above, no agreement will be needed for [redacted]*'s Purpose* because UP Diliman will be separated from [redacted]'s data processing for "additional features and services".

Please feel free to reach out for clarifications or further concerns.

Yours,

(Sgd.) Elson B. Manahan
Data Protection Officer
University of the Philippines Diliman

[22] See draft Outsourcing, Non-Disclosure and Data Protection Agreement attached to this Advisory Opinion.
[23] Implementing Rules and Regulations of the Data Privacy Act of 2012, Section 44.
[24] *Supra*, 6.
[25] *Supra,* 7.