Vol. 38 · October 2019
DOI: https://doi.org/10.7719/jpair.v38i1.733

Print ISSN 2012-3981
Online ISSN 2244-0445

Perceptions of Students, Faculty and Administrative Staff on the Data Privacy Act: An Exploratory Study

DAVID PAUL R. RAMOS
http://orcid.org/0000-0001-9663-6633
dprramos@plm.edu.ph
Pamantasan ng Lungsod ng Maynila
Gen. Luna cor. Muralla Sts., Intramuros, Manila

Originality: 100% • Grammar Check: 99% • Plagiarism: 0%

ABSTRACT

The Data Privacy Act of 2012 was enacted to "protect the fundamental human right of privacy of communication while ensuring a free flow of information to promote innovation and growth." Data privacy pertains to the right of an individual not to disclose his or her information. Since privacy is a universal human right, it is the responsibility of the government to protect the rights of its people to privacy and provide measures to protect their data. Given that the Data Privacy Act's implementation is a relatively recent development in the Philippines, little is known about the various stakeholders' perceptions towards it. A qualitative study which utilized semi-structured interviews was conducted to explore selected students', faculty members' and administrative staffs' perceptions of the Data Privacy Act. Non-probability, purposive sampling was used to recruit six respondents. An interview guide was developed to help in the facilitation of the interviews. Data were analyzed through the 6-step thematic analysis by Braun & Clarke (2006). Four themes emerged: 1) Limited awareness of the law, 2) Somewhat familiar with the purpose/ functions of the law, 3) Issues in the implementation of the law in the academe, and 4) Ambiguity in the necessity of the law. Recommendations to improve compliance with the Data

Privacy Act, such as the designation of personal information controllers or data privacy officers (DPO) to ensure that security measures are in place to protect personal and sensitive information, were also discussed.

Keywords **—** Data Privacy, Data Privacy Compliance, Qualitative study, Thematic Analysis, Manila, Philippines

INTRODUCTION

The enactment of the Data Privacy Act on September 9, 2016, was timely given the growing advent of modern technology and the increasing number of internet users, with approximately 4.5 billion internet users around the globe in 2019 (Internet World Stats, 2019). Almost 50% or roughly 2.3 billion of these internet users are Asians. Since Filipinos are heavy social media users and because of the rapid growth of the digital economy, strengthening Philippine's privacy and security protections is a welcome development.

On August 15, 2012, President Benigno C. Aquino III signed a law that penalizes unauthorized disclosure of personal information – Republic Act 10173 or The Data Privacy Act of 2012. The Data Privacy Act was enacted to "protect the fundamental human right of privacy of communication while ensuring a free flow of information to promote innovation and growth" (Republic Act. No. 10173, Ch. 1, Sec. 2). The law defines data privacy as the right of an individual not to disclose his or her information (Republic Act. No. 10173). It applies to individuals, corporations, organizations, and or legal entities that process personal information. The National Privacy Commission's (NPC) Circular Number 16-01 reminded all heads of government branches, including state universities and colleges, that the law applies to all government agencies, bodies or entities that are engaged in the processing of personal data (Doce & Ching, 2018).

International Privacy Standards

The Philippines' Data Privacy Act was patterned from international privacy standards. Some of the international accords related to privacy include the Asia Pacific Economic Cooperation (APEC) Privacy Framework (2004), European Data Protection Directive 95/46/EC, Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980, and the General Data Protection Regulation (Callo-Muller, 2018; Mattoo & Meltzer, 2018). The first version of

the APEC Privacy Framework of 2005 was aimed at implementing a "mechanism for mutual recognition or acceptance of different domestic privacy laws, which would allow for effective privacy protection without creating unnecessary barriers to cross-border information flows" (Callo-Muller, 2018).

The European Union (EU), however, implemented the General Data Protection Regulation, considered to be the "world's most comprehensive regime," replacing the 1995 data Protection Directive (Mattoo & Meltzer, 2018). The new GDPR is stricter, as it widens the scope and strengthens the enforcement of privacy standards by only allowing personal data out of the EU under strict conditions to protect privacy abroad – and that is if a non-EU country enacts privacy legislation that is equivalent to the GDPR (Mattoo & Meltzer, 2018). Although the new GDPR has a legitimate objective to protect privacy, it makes international data transfers more difficult, which could be problematic for some developing countries (Mattoo & Meltzer, 2018). The obligations contained in the GDPR have been characterized by many as being too stringent (Callo-Muller, 2018).

The GDPR applies to the processing (collection, use, and disclosure) of personal data of an identified or identifiable person (Callo-Muller, 2018). "Special categories" of personal data, such as genetic data, biometric data, health data, and data concerning a person's sex life or sexual orientation, are subject to stricter rules under the GDPR (Callo-Muller, 2018).

The ASEAN Member States, on the other hand, has developed a framework on personal data protection. The framework "serves to strengthen the protection of personal data in ASEAN and to facilitate cooperation among the Participants (Member States), to contribute to the promotion and growth of regional and global trade and the flow of information" (*Framework on Personal Data Protection*, 2016). The framework emphasizes the following principles: 1) consent, notification, and purpose; 2) accuracy of personal data; 3) security safeguards; 4) access and correction; 5) transfers to another country or territory; 6) retention; and 7) accountability.

These international accords and the existing challenges brought on by the rapidly advancing ICT are precursors to the establishment of the Data Privacy Act in the Philippines. RA 10173 was patterned after the GDPR (Ching, Fabito & Celis, 2018).

Establishment of the National Privacy Commission (NPC) in the Philippines

RA No. 10173 created the National Privacy Commission (NPC) under the Department of Information and Communications Technology (DICT), the agency that is mandated to enforce policies on data protection. The NPC was established to administer and implement the provisions of RA 10173, and to monitor and ensure compliance of the country with international standards set for data protection (Republic Act. No. 10173, Ch. 2, Sec. 7). Specifically, some of the functions of the NPC include: 1) ensuring the compliance of personal information controllers with the provisions of the Act, 2) receiving complaints, instituting investigations, facilitating or enabling settlement of complaints through the use of alternative dispute resolution processes, 3) monitoring the compliance of other government agencies or instrumentalities on their security and technical measures and recommend the necessary action to meet minimum standards for protection of personal information pursuant to this Act, and 4) ensuring proper and effective coordination with data privacy regulators in other countries and private accountability agents, among others (Republic Act. No. 10173, Ch. 2, Sec. 7).

Salient Features of the Data Privacy Act of 2012

RA 10173 applies to the processing of personal information and sensitive personal information. The law considers the following as sensitive personal information: the individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; health, education, genetic or sexual life of a person, or to any proceeding or any offense committed or alleged to have committed; issued by government agencies unique to an individual such social security number; and anything marked as classified by executive order or act of Congress (Wall, 2017). It is broadly applicable to individuals and legal entities that process personal information. Among other things, it created parameters on when and on what premise can data processing of personal information be allowed. The basic premise for when data collection and processing is allowed is when the data subject has given his/her direct consent.

Furthermore, it is the right of the data subject to know if his or her personal information is being processed and can demand information on how his or her personal information is being used. Institutions, both government and private, are mandated to assign personal information controllers who would ensure that security measures within their institutions are in place to protect the personal information of all stakeholders (Republic Act. No. 10173). Heads of government

agencies must, therefore, ensure that their system is compliant with the law. Penalties will be imposed regarding violations committed against the provisions of the law, such as unauthorized processing, unauthorized purposes, unauthorized access or the intentional breach, concealment of security breaches, negligence, and malicious and unauthorized disclosure (Republic Act. No. 10173). In case the data has been compromised, the personal information controllers must notify the data subjects affected and the National Privacy Commission (Republic Act. No. 10173). The challenge is for institutions to translate these provisions into practice.

Since privacy is a universal human right, it is the responsibility of the government to protect the rights of its people to privacy and provide measures to protect their personal data. Unfortunately, even if the Data Privacy Act has been passed, some institutions and organizations are not implementing the full provisions of the law. In a case study conducted on the Commission on Higher Education (CHED) and Commission on Elections (COMELEC), barriers to ensure compliance to the law includes lack of awareness, budget, and time constraints (Ching, Fabito & Celis, 2018). It is crucial and imperative that institutions provide measures to protect the interest of its employees with regard to their data. In line with this, the present study was conducted to explore selected students', faculty members' and administrative staffs' perceptions of the Data Privacy Act of 2012. It is aimed to gain a better understanding of the stakeholders' perceptions and awareness on the salient features of the law, its implementation, and its necessity. It also sought to gain insights into existing challenges and barriers in complying with the law. Given that the Data Privacy Act's implementation is a relatively recent development in the Philippines, little is known about the various stakeholders' perceptions towards it.

OBJECTIVES OF THE STUDY

The present study aimed to determine the respondents' perceptions of the Data Privacy Act of 2012 and explore the possible implications. It was intended to explore the students', faculty, and administrative staff's awareness of the law's functions, implementation and, a necessity in the academe. The following questions were asked (1) What are your perceptions on the Data Privacy Act of 2012?, (2) Do you know of any organizational, physical, and or technical security measures for personal data protection that is being implemented in your school/ workplace? (3) Do you think the Data Privacy Act of 2012 is necessary for your

school/workplace?, and (4) How do you think this law benefits the students/ faculty members/ administrative staffs in the university?

CONCEPTUAL FRAMEWORK

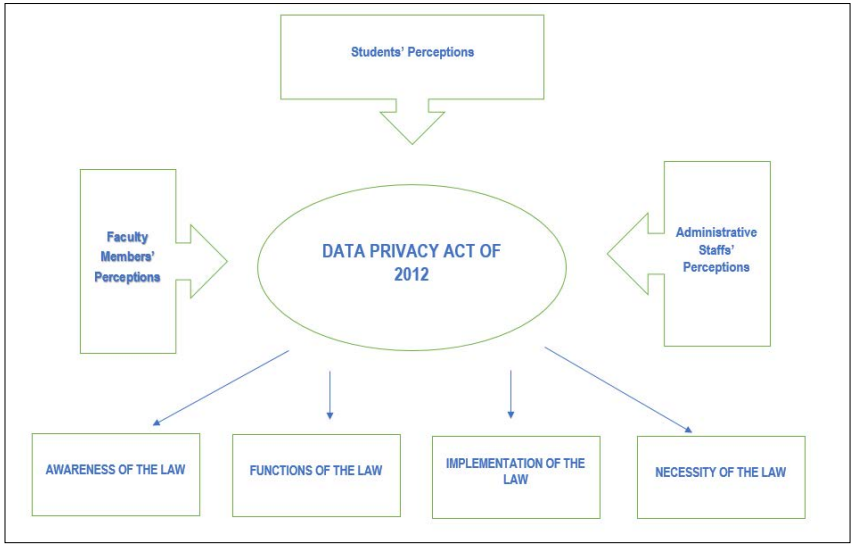

Figure 1. The Research Paradigm

METHODOLOGY

Research Design

The researcher utilized an exploratory research design that was done through the collection of qualitative data. Exploratory research designs are conducted when not much has been written about the topic or the population being studied, and the researcher seeks to listen to participants and build an understanding of what is heard (Creswell, 2014). The exploratory design was employed since both the topic and the population studied have not been thoroughly explored. Moreover, the researcher sought to have a deeper understanding of the respondents' perceptions. Qualitative data collection was done through open-ended, semi-structured interviews, which allowed the researcher to gain thick and rich verbal descriptions from the respondents regarding their viewpoint. Data were analyzed

through thematic analysis. Rigor and trustworthiness were observed through reading and rereading of transcripts and data, participant, and peer validation. Qualitative research is an approach for exploring and understanding the meaning of individuals or groups ascribe to a social or human problem (Creswell, 2014).

Research Site

The research was conducted in a local university in Manila, which involved students, faculty members, and administrative staff from the same institution.

Instrumentation

An interview guide with four open-ended questions was constructed for this study. The questions focused on exploring the students', faculty, and administrative staff's awareness of the law's functions, implementation, and necessity in the academe. Follow-up questions were also asked for clarifications.

Sample and Sampling Technique

A total of six respondents participated in the study – two faculty members, two administrative staffs, and two students. The study utilized non-probability, purposive sampling. The participants were informed of their rights to withdraw from the study at any point during the research process.

Data Gathering Procedure

Permission to conduct the interviews was secured from respective authorities. The collection of data was conducted through a semi-structured interview. An interview guide was prepared prior to data collection. Written consent to take part in the study was given and obtained from the respondents informing them of their rights to refuse to answer questions and to withdraw from the study at any point during the data collection process. The nature and purpose of the study were explained to the respondents at the onset. The recruitment of respondents was done through purposive sampling. The interviews were conducted in a mix of English and Tagalog. The respondents were allowed to discuss any questions or concerns about the study. A pseudonym for each respondent was used, and other measures to ensure anonymity and confidentiality were exercised.

Ethical Considerations

This research undertaking was committed to the highest standard of professional conduct. To meet the ethical requirements established for this study,

written consent was obtained from the participants informing them of their right to refuse questions or withdraw from the study at any time during the data collection process. The purpose of the study and methodology were explained to the participants. They were allowed to express their concerns about the study. Pseudonyms were used to ensure anonymity and confidentiality.

Data Analysis

The 6-step framework proposed by Braun & Clarke (2006) as an approach to thematic analysis was followed. Thematic analysis refers to the process of identifying patterns or themes within qualitative data (Braun & Clarke, 2006). The goal is to identify salient themes and patterns that are important and or interesting. Braun & Clarke's (2006) 6-step framework is considered one of the most influential approaches in conducting a thematic analysis in the social sciences (Maguire & Delahunt, 2017). The 6-step framework involves:

Step 1: Become familiar with the data
Step 2: Generate initial codes
Step 3: Search for themes
Step 4: Review themes
Step 5: Define themes
Step 6: Write-up

Transcripts of the interviews were read, re-read until a pattern emerges. To ensure credibility, participant validation was employed, where the researcher's analysis of the data was compared with the participants' accounts to establish a level of correspondence. To ensure validity, a colleague was asked to analyze the results to see whether the analysis of the data was accurate.

RESULTS AND DISCUSSION

The analysis of the data established four higher-order themes that encapsulated the respondents' perceptions of the Data Privacy Act of 2012. To present the structure of these perceptions, a table of the higher-order themes, subthemes, and an illustrative text was formed. The four higher-order themes are as follows:

1. Limited awareness of the law
2. Purpose/ functions of the law
3. Issues in the implementation of the law in the academe
4. Ambiguity in the necessity of the law

Table 1 lists the specific sub-themes and illustrative quotations for each of the higher-order themes.

Table 1. Superordinate Themes and Constituent Subthemes

Superordinate themes	Subthemes	Example of illustrative text
Limited awareness of the law	Somewhat familiar with the law	"I heard about it."
	The issue of informed consent	"According to it, *makukulong* ka if you didn't ask for informed consent."
Purpose/ functions of the law	Protection of sensitive personal information/ safeguarding of data	"It secures personal information."
	Regulation of data collection	"It prevents unlawful data collection, especially without the consent of the individual."
	Protection of the individual	"*Para na din sa proteksyon nung tao."*
Issues in implementation in the academe	Presence/absence of protective measures	"I don't know of any protective measures being implemented (in my school)."
	Presence/absence of department that regulates the implementation	"*Wala atang department na in-charge*."
Ambiguity in its necessity	Beneficial only in certain aspects	"I think it is beneficial in medical procedures, in insurance, in bank transactions."
	Gray areas	"*Medyo* vague *pa sya*. What if *magbabackground-check, pano yun*? What if age, sex, *lang yung* information need *pa din ng* informed consent?"

Theme 1. Limited awareness of the law

The responses of the participants ranged from "somewhat familiar" to "familiar" in terms of their awareness and familiarity with the law. When asked what they know about the law, most of the respondents said that it has something to do with informed consent:

"Yung data dapat di basta-basta nilalabas, dapat lagging may informed consent when asking for information." (Student 2)

"According to it, makukulong ka if you didn't ask for informed consent." (Faculty 1)

"This law secures the collecting and or gathering of sensitive personal information and the right to informed consent. (Faculty 2)

This indicates limited awareness of the law. There are many more salient features of the law that is not just limited to informed consent, such as the importance of parameters on when and on what premise can data processing of personal information be allowed where the basic premise is when a data subject has given direct consent (Section 12 and 13). The law also has provisions for companies who subcontract the processing of personal information to the third party, implicating that they shall have full liability and cannot pass the accountability of such responsibility (Section 14), among other provisions. This limited awareness has great implications. This may imply that the institution is not fully compliant with the law. This partial compliance of an educational institution is similar to the case analysis conducted by Doce & Ching (2018) on the compliance of a state university in Mindanao, where it was found not fully compliant to RA 10173, although great efforts are being exerted in maintaining its information management systems and internet usage (Doce & Ching, 2018).

Theme 2. Somewhat familiar with the purpose/ functions of the law

The respondents' perceptions on the purpose/ functions of the law were centered into three subthemes, 1) Protection of sensitive personal information/ safeguarding of data, 2) Regulation of data collection, and 3) Protection of the individual:

"It is there for safekeeping of important records." (Admin staff 1)

"For the protection of the students and staff and of the university." (Faculty 1)

"It ensures that sensitive information is protected and before any information can be taken from an individual, that individual has to provide his or her voluntary consent." (Faculty 2)

This is consistent with the rationale of why the law was created. The law applies to the processing of personal information (section 3G) and sensitive personal information (Section 3L) and protects the right to privacy and prevention of unlawful data collection.

Some of the respondents agreed that the law is for the protection of the individual. This might be explained by their knowledge of the provision of the law that states that data subjects have the right to know if their personal information is being processed and that they can demand information such as the source of info, how their personal information is being used, and a copy of their information. Some of the respondents were also aware that they have the right to request removal and destruction of one's personal data unless there is a legal obligation that required for it to be kept or processed. (Section 16 and 18). However, this knowledge, which is at best incomplete, might not be due to the efforts conducted by the institution.

Theme 3. Issues in the implementation in the academe

All of the respondents mentioned that they do not know of any organizational, physical, and or technical security measures for personal data protection that is being implemented in the school:

"None that I know of." (Faculty 1)

"There were no concrete procedures or manifestations of its implementation. (Faculty 2)

"Parang wala naman." (Admin staff 1)

"Hindi ko po alam kung meron." (Admin staff 2)

"I think none po." (Student 1)

"Wala po akong alam." (Student 2)

This awareness or the lack thereof any organizational, physical, and or technical security measures for personal data protection that is being implemented in the school has great implications. The National Privacy Commission was created to monitor the implementation of this law (Section 7). It is the duty of the NPC to ensure that all organizations, both government and private, implement the provisions as stated in the law. The NPC should, therefore, exert more effort in ensuring that all institutions abide by the law. On an institutional level, all institutions are mandated to provide protective measures to ensure the protection of sensitive personal information and lawful data collection and processing. The institution should make sure that its students, faculty, and administrative staffs are well-informed of how they are implementing the law. Furthermore, not one of the respondents were familiar if the institution has designated a data privacy officer.

Barriers and challenges may prevent the institution from fully complying with the law. However, individuals who were in authority to answer were not tapped for an interview. In the case of one state university, factors that contribute to partial compliance include a lack of better understanding, budgetary issues, and time constraints (Doce & Ching, 2018). Lack of better understanding was said to have emanated from not getting everyone involved in the initiative of protecting university data across all units (Doce & Ching, 2018). Similarly, two government institutions reiterated three factors that hamper their compliance: lack of awareness, budget, and time constraints (Ching, Fabito & Celis, 2018).

Theme 4. Ambiguity in its necessity

Although most of the respondents have positive attitudes towards the Data Privacy Act of 2012, some of them mentioned that there are still "gray areas":

"Medyo vague pa sya." (Student 2)

"Beneficial for medical purposes and for students undergoing counseling, but other than that, it's not clear to me." (Student 1)

"Sa banking records, for insurance, for medical records, not sure po sa ibang bagay." (Admin staff 1)

The Implementing Rules and Regulations of the Data Privacy Act of 2012 aims to clarify these ambiguities not just in its necessity, but also in its implementation. Awareness of its importance and the How's of its implementation should be made known to individuals in the academe. Undoubtedly, protecting personal information is necessary. In light of the continuously changing information technology, and how it affects our daily living, concerns regarding data protection and usage are becoming more evident (Xu, Teo & Tan, 2006).

CONCLUSIONS

The study contributes to the literature by providing inputs about the institution's efforts in implementing the law. This study also provided insights into the implications of students' and employees' perceptions of the Data Privacy Act of 2012 and the compliance of the institution in implementing the law. The respondents were clearly just somewhat familiar, if not unfamiliar with the provisions of the law, its functions, and necessity. The institution where the respondents belong to should exert greater effort in making their constituents become more aware and actively participate in the protection of privacy. More

effort is needed so that the information that they know about the law is not just limited to informed consent. Also, in terms of implementation, not one respondent mentioned that they were aware of any steps or procedures being undertaken by the institution with regards to complying with the law. Institutions have to take a more active role in terms of compliance with the law and how this will affect all stakeholders. Furthermore, the National Privacy Commission should intensify its efforts in ensuring that all government and private institutions are compliant with the law.

Given that most of the respondents are unfamiliar with the salient features of the law and its implementation in the university, it becomes a challenge for the university to comply. There is a need to assess possible data privacy risks occurring within the university, implement protection strategies and how they will be implemented, and to prepare for the different forms of breaches or violations of the law within the bounds of the university. There should be an active commitment to comply with protecting the rights of the individual to privacy – from protecting the individual's right to be informed, to ensuring that the data collected from the individual is secured and properly stored.

Since the Data Privacy Act is relatively new in the Philippines, very few researchers have been conducted both in government and private institutions; hence, the results of this exploratory research can be used as a basis for future researches and policymaking. One limitation of the present study is that other stakeholders, such as the institution's officials, members of the Administration, and third parties were not included in the study.

TRANSLATIONAL RESEARCH

Based on the results of the present study, recommendations to strengthen the compliance on data privacy protection in the academe were deemed necessary to improve the university policy on data privacy and ensure data privacy protection. A proposed institutional guideline on data privacy act compliance was developed to improve the security measures of the university. The institutional guideline involves primarily the designation of personal information controllers or data privacy officer (DPO) to ensure that security measures are in place to protect personal and sensitive information. The DPO should be tasked to ensure that the university is compliant with the law. An analysis of the type of data that the institution collects and stores is also necessary. *What type of data is being collected and stored by the institution, and what measures are needed to protect them?*

The integration of appropriate maintenance and management of data should be introduced into the working practices of the user population. Provisions for specific departments, such as the Office of the Guidance and Testing Services, University Health Services, and Office of the University Registrar, should be subject to the principles of transparency, proportionality, and for a legitimate purpose. To ensure commitment that all stakeholders comply with data privacy policies, awareness campaigns and data privacy trainings should be regularly conducted. Furthermore, periodic auditing of the state of compliance should be implemented and continuously strive to achieve compliance through frequent monitoring risks and by keeping all stakeholders informed.

Central to the proposed institutional guideline is an appropriate collection of information, privacy principles, provisions for specific departments/units, use and disclosure of information and security measures:

Collection of Information

The privacy principles of transparency, proportionality, and for legitimate use should always be followed. Transparency refers to obtaining the data subject's consent before collecting the information and informing him/her of the purpose for which the information is to be collected. Proportionality refers to only collecting information that is reasonably necessary or directly related to university functions. In collecting personal information, the university shall use the information only for legitimate purposes. Personal information such as student's name, parents' name and addresses and contact numbers, etc., for example, shall be used only for purposes such as enrolment and academic activities.

Security Measures

In line with the university's mandate to comply with the DPA and its IRR to secure the personal information of its students, parents, employees and third parties, the university shall designate its Data Privacy Officer (DPO) or a personal information controller, who is tasked to designated to monitor and ensure the implementation of the DPA and its IRR and the Data Privacy policies of the School. Members of the Data Privacy Office shall also be designated. The DPO is the de-facto head of the Data Privacy Office, which is tasked to respond to inquiries and complaints relating to data privacy and to assist in the monitoring and implementation of the Data Privacy policy of the university. The university shall create a Data Privacy Manual, which contains data privacy policies which shall be reviewed annually and regularly updated. The university

shall regularly conduct awareness campaigns and data privacy training as part of its commitment to ensuring that all its students and employees comply with its data privacy policies. To ensure that the potential privacy impact of the university's processes, information system programs, and other initiatives that process personal information of students, employees, and third parties are evaluated, privacy impact assessments are conducted for such projects, programs, and initiatives.

The university shall also take reasonable steps to protect the personal information in its possession from misuse, loss or unauthorized access, modification, or disclosure. As most of the personal information of students and employees is stored in the university databases, access to personal information in digital or digitized form by authorized IT personnel is restricted and individually identifiable. An approval process is in place for internal requests (i.e., special requests for authority to view student profile for disciplinary cases, counseling, or health concerns) for access to restricted student or employee records contained in the university information systems. As a general rule, only authorized personnel with the necessary approvals may request access to the information systems of personal information. Physical access to the servers and network equipment is highly restricted to authorized personnel only. Various security appliances and devices shall be employed to safeguard the university network and its systems.

Access to student and employee personal information is limited to authorized personnel of the specific departments collecting or processing the information. Aside from access restriction, the storage facilities for the hard copies of documents containing personal information shall also be secured. Only authorized personnel can open or have access to keys to the storage facilities. The storage units or facilities are placed in areas that are not usually accessible to the public, safe from physical hazards such as rain, wind, and dust, and located in areas that are usually manned by the authorized personnel.

Only authorized personnel shall have access to student or employee personal information. Students or parents or guardians (in case of minors) who wish to have access to their own personal information may submit a written request directly to the Registrar's Office and may be allowed access to their specific individual information or given copies, pursuant to the policies and guidelines on requesting for access or copies of student records. Requests for information through telephone will not be allowed.

Employees who wish to view their personal information in their individual personnel file may file a written request or directly go to the HRD Office, and

request for viewing of such information in the presence of authorized personnel of the department. In such cases where any individual or entity (other than the student, parent or guardian in case of minors, or employee) wishes to have access pursuant to the instances or exceptions provided under Data Privacy Act, a written request shall be submitted to the Department Head who may either endorse or reject the same. If approved, the endorsed request shall be submitted to the DPO or her duly authorized representative for approval. Only written requests properly endorsed by the Department Head shall be considered for approval.

In cases where government agencies empowered under the law to request for personal information (i.e., BIR, DOH), request for access, university personnel must ensure that the request is in writing, citing the authority upon which the request is made. In cases where the request is a result of a valid order or decision of a tribunal or court, a copy of such order shall be attached to the written request. Once approved by the DPO, it shall be transmitted to the Department Head or appropriate Department for implementation. The Department Head, who endorsed the same shall be responsible for monitoring compliance of the requestor on the terms of the approved request (i.e., time limit and confidentiality). In case there is a doubt on the propriety of any request for access, university personnel should consult or seek clearance from the Legal Affairs Department or the DPO.

The university is recommended to create a policy on how long it shall keep the student and employee records, including the information contained therein. No personal information may be destroyed unless allowed by certain laws, and such destruction, if allowed or authorized by law and the university, must be documented in writing by the university. Unauthorized destruction should be reported to the DPO or any member of the Data Privacy Office.

Provisions for Specific Departments

The Office of the University Registrar (OUR) shall only collect personal information for the purpose of evaluating the eligibility of the applicant for admission or in case of current students, for enrollment in the School; for the purpose of providing placement services required on the job training for students; and evaluation of students for eligibility for scholarships provided by the university and third parties.

The information collected by the Office of the Guidance and Testing Services shall be processed only by authorized personnel and for legitimate purposes of the university. In the course of the collection of information, this authorized

personnel from these offices ask data to fill out forms with the corresponding privacy statement to signify consent and to inform them of the purpose of collecting such information during the admission and or enrollment processes. Only authorized personnel are allowed to encode and access student data.

The Human Resource Department shall collect information from employees or applicants for purposes of evaluating the applicant for eligibility for employment, and to avail of employee benefits (i.e., retirement, educational, and medical benefits). Pursuant to existing labor laws and human resources policies of the university, the 201 files or employee's individual employment records are confidential, and access is restricted to authorized personnel only.

Access to the data collected by the University Health Services is restricted and limited only to authorized personnel in the department, such as the school doctor, dentist, or nurse assigned in the Department. Sensitive information may not be released without the prior consent of the student or guardian except in the life case of the student, or other students (i.e., epidemic cases as provided under the DOH rules and regulations) is at stake.

In all instances, any access to personal information of students must be with their or their parents/ guardians' consent, or employee's and for legitimate purposes, or endorsed by the Department head.

Privacy Policies

To ensure that the rights of the data subjects are protected, the above-mentioned departments are subject to the following policies: 1) data subjects are notified and their consent secured: 2) only authorized personnel are allowed to access and process the personal information collected from the students, their parents or guardians and that student records as well as the information contained therein are to be kept confidential; and 3) information that will be collected is reasonably necessary and directly related to university functions or purposes.

LITERATURE CITED

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77-101. Retrieved from DOI: 10.1191/1478088706qp063oa

Callo-Muller, M. V. (2018). APEC Policy Support Unit, Policy Brief No. 23: GDPR and CBPR: Reconciling Personal Data Protection and Trade. Retrieve from http://bit.ly/2OtXmne

Ching, M. R. D., Fabito, B. S., & Celis, N. J. (2018). Data Privacy Act of 2012: A Case Study Approach to Philippine Government Agencies Compliance. *Advanced Science Letters*, *24*(10), 7042-7046. Retrieved from https://doi.org/10.1166/asl.2018.12404

Creswell, J. W. (2014). *Research design: Qualitative, quantitative and mixed methods approach* (4th ed.). Thousand Oaks, CA: SAGE Publications.

Creswell, J. W. (2014). Qualitative inquiry and research design. Retrieved from http://www.ceil-conicet.gov.ar/wp-content/uploads/2018/04/CRESWELLQualitative-Inquary-and-Research-Design-Creswell.pdf

Doce, L. J. & Ching, M. R. (2018). RA 10173 and it challenges to universities and colleges' compliance performance: The case of Mindanao State University – General Santos City. DOI: http://doi.org/10.1145/3234781.3234789

Framework on Personal Data Protection (2016). ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN), Bandar Seri Begawan, Brunei Darussalam.

Internet World Stats (2019). Retrieved from https://www.internetworldstats.com/stats.htm

Maguire, M., & Delahunt, B. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *AISHE-J: The All Ireland Journal of Teaching and Learning in Higher Education*, *9*(3). Retrieved from http://bit.ly/31Vs4JR=

Mattoo, A. & Meltzer, J. P. (2018). International data flows and privacy: The conflict and its resolution. *Journal of International Economic Law*, 21, 769-789. Retrieved from https://doi.org/10.1093/jiel/jgy044

Republic Act 10173 – Data Privacy Act of 2012. National Privacy Commission. Retrieved from https://www.privacy.gov.ph/data-privacy-act/

Wall, A. (2017 April 27). Summary: Philippines Data Privacy Act and implementing regulations. Retrieved from http://bit.ly/2IvBKmA

Xu, H., Teo, H. H., & Tan, B. (2006). Information privacy in the digital era: an exploratory research framework. *AMCIS 2006 Proceedings*, 120. Retrieved from http://bit.ly/35RXWRO