Asian Journal of Multidisciplinary Studies
Vol. 4, No. 2, (2021)
ISSN 2651-6691 (Print)
ISSN 2651-6705 (Online)

The Implementation of the Data Privacy Act among Higher Educational Institutions in the Province of Pangasinan

Clark Kim C. Castro[1]
[1] Faculty, Pangasinan State University Lingayen Campus College of Computing Sciences

Abstract *– Data is the most important asset of an organization. As such, they are vulnerable to breaches and requires regulation to compel organizations to establish frameworks that assure the data owners of safety. In the Philippines, the Republic Act (RA) No. 10173 or also knows as "Data Privacy Act of 2012" (DPA of 2012) was signed into law creating the National Privacy Commission (NPC) to promote, regulate, and monitor data privacy compliance of both government agencies and private institutions. This study sought to assess the extent of implementation of Republic Act 10173 or otherwise known as the Data Privacy Act in higher educational institutions (HEIs) and determine the roadblocks within and outside HEIs that contributed to challenges in its implementation. Sampling sixty (60) employees across ten (10) HEIs, both public and private, the researchers found that the Data Privacy Act is Moderately Implemented in HEIs with an Overall AWM of 2.92. Among the most serious issues that encountered were found to be in terms of compliance to Data Breach Notification and Registration and Compliance Requirements.*

Keywords – RA 10173, Data Privacy Act, Data Privacy Implementation, Higher Educational Institutions, HEIs

INTRODUCTION

Data is the most important asset of any institution it may be public nor private. The financial value of data is such that individual privacy is often set aside in the pursuit of commercial advantage.[1] Today, the world is the age of digital information revolution. Technology has already conquered the worlds processing mechanism, IR (Industrial Revolution) 4.0 and IOT (Internet of Things). Everyone relies in using technology-based equipment and machineries. Also, internet, a technological breakthrough, has done a big changed in business, government and even to every individual. No one can live already without using internet. It provides everything, all information needed, entertainment to enjoy like games, music and movies, meeting new friends, and even government and business process uses the internet. Big data is already coming up because everyone already uses technology platforms, in which there is a bulk of data processing being done to create information to be used. As to the application of the IR 4.0, machines will transfer data to be manipulated and converted to a process on how it will work and perform the communicated service.[2]

Before the widespread adoption of digital information, information was generally held in discrete and often poorly catalogued packets. All processes must be placed in paper where it will be kept in large cabinets for archiving and storage. This was the practice for how many years where technology was not yet that revolutionized. The old age was been time consuming and expensive in a way that more facilities and equipment are needed to perform the task. These are the reasons why technology changes fast and unmeasurable on how it will end. Technology evolution is one of the unsatisfying factors of human behavior. Odds of this enhancement has been reflected to the current situation of the world. Some provided good services, others made other people suffered.

The majority of government agencies and national institutions promote good democratic governance by providing transparent and accountable civic information based on citizen data. As a result, appropriate precautions must be taken in the collection, provision, and sharing of such information in order to safeguard and protect each individual's privacy. Data protection and privacy have long been a source of concern in terms of how security and data proliferation must be appropriately shared, accessed, and, most importantly, protected. [3]

Countries and organizations work to develop provisions, laws, and even amendments to protect the personal information of all individuals on a global scale. [3] It is very important to protect personal information as it represents the private description of one individual. The information may be used to access the personal belongings and other takings. Personal data is an information that relates to an identified or identifiable individual, according to the European Commission. An individual that cannot be directly identify from the information given, he/she is considered identifiable. Take into account the information that will be process with all the means reasonably likely to be used by either you or any other person to identify that individual. [4]

Data Protection Authorities (DPAs) in the European Union (EU) are an independent body with a primary role in data privacy and protection that legally enforces a binding commitment on data privacy and security. While the General Data Protection Regulation (GDPR), which is also a regulating body that monitors and enforces data protection action among organizations including private institutions, plays a leading role in data privacy regulation and recognizes compliant entities.[3][5]

The European Commission have identified twelve (12) countries outside the EU that offers an adequate level of data protection. The countries are Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay while South Korea is still under adequacy talks. [6]

In US, there is no single principal data protection legislation, instead hundreds of laws enacted in both federal and state level for the security of the personal information of the US residents. [7]In July 06, 2017 at the G7 Ise Shima Summit in Brussels, Japan adapted the EU General Data Protection Regulation (GDPR) on 24 May 2016, which was applied from 25 May 2018, and of the Japanese Act on the Protection of Personal Information (APPI) on 30 May 2017, the EU and Japan have further increased the convergence between their two systems, which rest notably on an overarching privacy law, a core set of individual rights and enforcement by independent supervisory authorities. [4]

In Philippines, to safeguard the process, it created and established the Republic Act (RA) No. 10173 or also knows as “Data Privacy Act of 2012” (DPA of 2012). This established the National Privacy Commission (NPC) to promote, regulate, and monitor data privacy compliance of both government agencies and private institutions benchmarked with international standards set for data protection which patterned in the EU's GDPR.[3] [8]It was observed that most of the data was unprotected and prone to any data breach. An example incident happened last March 20 to 27, 2016 in the country, where 76,678,750 personal information of Filipino voters were leaked under the office of Commission of Elections (COMELEC). This could have been prevented if only the COMELEC complied with the necessary requirements of the DPA 2012 and provided an Information Security Management System (ISMS). [9][10]

The government is working hard to prevent different unusual process that could harm the public interest. The country's frontline agency in the provision of employment, labor workforce information, and services; protecting and promoting the welfare and interests of every citizen to work locally and globally has fully utilized its ICT infrastructure to ensure broader public access to information. Furthermore, provide comfortable, convenient, and efficient processes, and seeks to realize a governance system that will lead to faster and better delivery of goods and services, as well as proactive citizen participation in management. It provides a variety of services to Filipinos and collects and stores personal information.[3]

HEI's especially private institution needs to comply the needed requirements for them to protect and safeguard their operations to sustain their process and not to affect their business transactions since its financial capability depends on its number of students being catered.[11] [12]The proponent would like to study the implementation of Republic Act (RA) No. 10173 or also knows as "Data Privacy Act of 2012" (DPA of 2012) in selected Higher Educational Institutions (HEI's) in Pangasinan.[8] HEI's handles millions of data, it collects, process and provide information to its students and clienteles.

OBJECTIVES OF THE STUDY

This study sought to assess the extent of implementation of Republic Act 10173 or otherwise known as the Data Privacy Act in higher educational institutions and determine the roadblocks within and outside HEIs that contributed to challenges in its implementation. Specifically, the study sought to answer the following questions:

1. What is the profile of the higher educational institutions (HEIs) in the province of Pangasinan?
2. What is the profile of the respondents?
3. What is the extent of implementation of the Data Privacy Act in the HEIs?
4. What are the problems encountered in the implementation of the Data Privacy Act in the HEIs?

METHODOLOGY

This study employed a descriptive research design. The respondents of the study are sixty (60) employees of public and private higher educational institutions in the province of Pangasinan. Purposive sampling was used for the selection of respondents in the study. The respondents are either data privacy officers, process owners or information systems personnel of the HEIs. The researchers used a survey questionnaire for gathering data from the respondents. [13]The questionnaire has constructed by the researchers with two parts. The first part asks for the profile of the respondents and the second part is composed of questions derived from the Data Privacy Act and the most encountered problems found in literature review. [8]A Likert-scale rating was used to gauge the awareness and the perceived level of implementation of Data Privacy Act among the respondents. The questionnaire was distributed to selected HEIs and asked to be distributed to the identified employees. The HEIs were given two weeks to accomplish the instrument and was retrieved by the respondents for encoding. The data was encoded into Microsoft Excel. Erroneous and incomplete data entries invalidated some responses and were removed from the final sample. The cleaned data was encoded and imported into IBM SPSS for analysis. Frequency, average weighted mean (AWM), and ranks were employed in data analysis.

RESULTS AND DISCUSSION

This section presents and discusses the results of the analysis conducted on the data collected from the employees of HEIs in the province of Pangasinan. Table 1 presents the profile of the HEIs covered in the study which includes the number of years of operation, number of enrollees assigned data privacy officers (DPOs), and total employees. Based on the results of the study, half of the HEIs in the province have been operating between 41-50 years. Six out of 10 HEIs have 5,001-10,000 students. Half of them have no assigned data privacy officers (DPOs), and half of them have 101-200 employees. This implies that only half of the HEIs have adhered to the first pillar of Data Privacy, which is to have somebody oversee their compliance with RA 10173 and registered in NPC their data processing system. [14][15]

Table 1. Profile of the Higher Educational Institutions

Variable	Category	Frequency	%
Number of Years of Operation	31-40 years	1	10%
	41-50 years	5	50%
	51+ years	4	40%
Number of Enrollees	5,001-10,000	6	60%
	10,001-15,000	3	30%
	15,001+ enrollees	1	10%
Assigned DPOs	None	5	50%
	1	3	30%
	2	1	10%
	>2	1	10%
Total employees	< 100	1	10%
	101-200	5	50%
	201-300	3	30%
	>300 employees	1	10%

Table 2 presents the profile of the respondents namely the employees of the HEIs based on their age, sex, position and number of relevant trainings attended. Based on the study, most of the respondents 25 or 41.67% of the employees are aged 35-44, a majority of them 41 or 68.33% are Male, 33 or 55% are non-teaching and all have received trainings related to data privacy. This reflects that the IT industry even within the academe is heavily dominated by male employees. This reaffirms the gap in IT jobs between men and women. The appointment of a data protection officer is deemed to be the easiest to comply with among the pillars of data privacy. [7]

Table 2 . Profile of the Respondents

Variable	Category	Frequency	%
Age	18-24 years old	3	5%
	25-34 years old	23	38.33%
	35-44 years old	25	41.67%
	45-54 years old	5	8.33%
	55+ years old	4	6.67%
Sex	Male	41	68.33%
	Female	19	31.67%
Position	Teaching	27	45%
	Non-Teaching	33	55%
Number of Trainings Attended	1-5	60	100%

Table 3 presents the level of implementation of the Data Privacy Act in the Province of Pangasinan as perceived by the employees. Based on the results, the overall AWM is 2.92 which implies that the employees perceive that the Data Privacy Act is Moderately Implemented in their respective institutions. Of the twenty-three (23) dimensions of implementation that are included two (2) areas were identified to have be Highly Implemented, seventeen (17) to be Moderately Implemented and four (4) areas to have AWMs perceived to be only Slightly Implemented. The reason why the HEIs adhere and comply to the mandate of the data privacy act is mainly due to legitimacy, deterrence and reputation. Government agencies, just like state universities, are expected to follow whatever the law dictates. [16][17]

The items "Right to Rectification" and "Physical Security Measures" incurred the highest AWMs with 3.61 and 3.42 respectively. This implies that the HEIs ensure that data owners will be able to correct their information should there be any changes or mistakes that may occur in the data that has been entered. Further, the HEIs have also invested in making sure that areas where data are stored physically are reinforced with heightened security to prevent any damage, breach or loss. This can also be attributed to the fact that data subjects have a great knowledge of their rights to correct any kind of inaccuracy or error regarding their personal information. This contrast in terms of right to rectify and right to suspend or withdraw their data is aligned to the study of Tanate-Lazo and Cabonero (2021). [18]

On the other hand, the respondents perceived the items "Right to Erasure or Blocking", "Data Breach Notification", "Breach Report", and "Registration of Personal Data Processing Systems" to have the lowest level of implementation with AWMs of 2.32, 2.28, 2.22, and 2.18 respectively. This shows that the HEIs have not fully committed to keeping their stakeholders informed in case of a breach of their personal data. This can be attributed to the deterrence on the part of HEIs emanating from legal risks that may come from the data owners. Responsible personnel are also held accountable in case of data breaches. With regards to the need to register personal data processing systems, it was determined that the system does not pose that much of a risk to the rights and freedoms of the data subject. Hence, the level of implementation in that area is low. This result actually aligns with findings made from other state universities such as Caraga State University which shows that breach notification procedure is not yet complied with. [17]Similarly, state universities such as Mindanao State University in General Santos and Bukidnon State University are also found to be partially compliant.[19][20] Institutions such as CHED and COMELEC, as of 2018, also have to comply with more requirements mandated by NPC to realize the full implementation of data privacy regulation in their respective offices.[14]

Table 3. Level of Implementation of the Data Privacy Act in HEIs in the Province of Pangasinan (n=60)

Items	AWM	Descriptive Equivalent	Rank
Organizational Security Measures	3.19	MI	5
Data Protection Policies	3.08	MI	11
Records of Processing Activities	3.10	MI	9
Management of Human Resources	3.06	MI	12
Processing of Personal Data	3.10	MI	9
Contracts with Personal Information Processors	3.28	MI	3.5
Physical Security Measures	3.42	HI	2
Technical Security Measures	3.06	MI	12
Right to be Informed	3.17	MI	7
Right to Object	2.91	MI	14
Right to Rectification	3.61	HI	1
Right to Erasure or Blocking	2.32	SI	20
Right to Damages	3.28	MI	3.5
Data Breach Notification	2.28	SI	21
Breach Report	2.22	SI	22
Subcontract of Personal Data	3.14	MI	8
Enforcement of DPA	2.68	MI	19
Registration of Personal Data Processing Systems	2.18	SI	23
Notification of Automated Processing Operations	2.75	MI	17
Accountability for Transfer of Personal Data	3.18	MI	6
Responsibility of Heads of Agencies	2.72	MI	18
Requirements Relating to Access by Agency Personnel to Sensitive Personal Information (Online and Onsite Access)	2.88	MI	15
Requirements Relating to Access by Agency Personnel to Sensitive Personal Information (Offsite Access)	2.85	MI	16
Overall AWM	**2.92**	**MI**	

LEGEND: 4.21-5.00 – Very Highly Implemented (VHI); 3.41-4.20 – Highly Implemented (HI); 2.61-3.40 – Moderately Implemented (MI); 1.81-2.60 - Slightly Implemented (SI); 1.00-1.80 – Not Implemented (NI)

Table 4 presents the results of the level of seriousness of the problems encountered in the implementation of the Data Privacy Act as perceived by the respondents from the HEIs. Overall, the problems encountered in implementation of DPA incurred an AWM of 3.24 which implies that the problems were found to be Moderately Serious. Two areas were found to have AWMs that can be interpreted as Highly Serious, while the rest have AWMs deemed to be Moderately Serious. The most serious problems were found to occur in terms of Data Breach Notification and Registration and Compliance Requirements which incurred an AWM of 3.72 interpreted as Highly Serious. The problems arising from data breach notification can be attributed to factors such as lack of awareness, lack of resources, and low priority in the agenda are found to be critical factors in complying with DPA of 2012. [20]The issue on registration and compliance can be attributed to issues arising from lack of budget, lack of understanding, and time constraint. [17]

Table 4. Problems Encountered in the Implementation of the Data Privacy Act in HEIs in the Province of Pangasinan (n=60)

Items	AWM	Descriptive Equivalent	Rank
Security Measures for the Protection of Personal Data	3.25	MS	3
Rights of Data Subjects	2.97	MS	6
Data Breach Notification	3.72	HS	1.5
Outsourcing and Subcontracting Agreements	3.03	MS	5
Registration and Compliance Requirements	3.72	HS	1.5
Rules of Accountability	2.85	MS	7
Security of Sensitive Personal Information	3.16	MS	4
Overall AWM	3.24	MS	

LEGEND: 4.21-5.00 – Very Highly Serious (VHS); 3.41-4.20 – Highly Serious (HS); 2.61-3.40 – Moderately Serious (MS); 1.81-2.60 - Slightly Serious (SS); 1.00-1.80 – Not Serious (NS)

CONCLUSION AND RECOMMENDATION

Based on the results of the study most of the respondents are aged 25-44 years old, Male, non-teaching and have received relevant trainings regarding data privacy. All of the HEIs have hundreds of employees and thousands of students, which makes the implementation of the Data Privacy Act highly necessary. It was found that HEIs were moderately implementing the mandate of DPA. Among the areas which require particular focus is in terms of Data Breach Notification and Registration and Compliance Requirements. Full implementation of the HEIs can be achieved if these challenges can be addressed. First, assigning their Data Protection Officers is one step in overcoming issues with compliance. Assigning an employee who will oversee the institution's compliance to RA 10173 is one step closer to better implementation. Moreover, a Data Privacy Manual must also be adopted and align practices across all HEIs.

REFERENCES

[1] S. Spiekermann, A. Acquisti, R. Böhme, and K.-L. Hui, "The challenges of personal data markets and privacy," *Electronic Markets*, vol. 25, no. 2, pp. 161–167, Jun. 2015, doi: 10.1007/s12525-015-0191-0.

[2] S. Yadav, A. Kaushik, M. Sharma, and S. Sharma, "Disruptive Technologies in Smart Farming: An Expanded View with Sentiment Analysis," *AgriEngineering*, vol. 4, no. 2, pp. 424–460, May 2021, doi: 10.3390/agriengineering4020029.

[3] V. Pitogo, "National Government Agency's Compliance on Data Privacy Act of 2012 a Case Study," *Journal of Physics: Conference Series*, vol. 1201, no. 1, p. 012021, May 2019, doi: 10.1088/1742-6596/1201/1/012021.

[4] G. Greenleaf, "The influence of European data privacy standards outside Europe: implications for globalization of Convention 108," *International Data Privacy Law*, vol. 2, no. 2, pp. 68–92, May 2012, doi: 10.1093/idpl/ips006.

[5] R. Rodrigues, D. Barnard-Wills, P. de Hert, and V. Papakonstantinou, "The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR," *International Review of Law, Computers & Technology*, vol. 30, no. 3, pp. 248–270, Sep. 2016, doi: 10.1080/13600869.2016.1189737.

[6] D. Barnard-Wills, C. Pauner Chulvi, and P. de Hert, "Data protection authority perspectives on the impact of data protection reform on cooperation in the EU," *Computer Law & Security Review*, vol. 32, no. 4, pp. 587–598, Aug. 2016, doi: 10.1016/j.clsr.2016.05.006.

[7] J. (Sophia) Baik, "Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA)," *Telematics and Informatics*, vol. 52, p. 101431, Sep. 2020, doi: 10.1016/j.tele.2020.101431.

[8] Republic Act 10173, *Data Privacy Act of 2012*. Congress of the Philippines, 2012.

[9] M. R. D. Ching and N. J. Celis, "Data privacy act of 2012 compliance performance of Philippine government agencies," in *Proceedings of the 2nd International Conference on E-commerce, E-Business and E-Government - ICEEG '18*, 2018, pp. 59–63. doi: 10.1145/3234781.3234784.

[10] M. R. D. Ching, B. S. Fabito, and N. J. Celis, "Data Privacy Act of 2012: A Case Study Approach to Philippine Government Agencies Compliance," *Advanced Science Letters*, vol. 24, no. 10, pp. 7042–7046, Oct. 2018, doi: 10.1166/asl.2018.12404.

[11] P. Queroda, "INTERNATIONALIZATION PERSPECTIVE OF PANGASINAN STATE UNIVERSITY: OPEN UNIVERSITY SYSTEMS," *Turkish*

Online Journal of Distance Education, 2020, [Online]. Available: https://dergipark.org.tr/en/pub/tojde/issue/55722/761931

[12] V. L. Uskov, J. P. Bakken, R. J. Howlett, and L. C. Jain, *Smart universities: concepts, systems, and technologies*. books.google.com, 2017. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=fYEkDwAAQBAJ&oi=fnd&pg=PR5&dq=smart+campus+literature+review&ots=gfgbm7FJ20&sig=l1tNunH9RX1zV0BKv9Oojz4yYSQ

[13] J. Bloomfield and M. J. Fisher, "Quantitative research design," *Journal of the Australasian Rehabilitation Nurses Association*, 2019.

[14] E. C. Gonzales and M. R. D. Ching, "Performance compliance of Philippine national government agency on the data privacy act of 2012," in *Proceedings of the 2nd International Conference on E-commerce, E-Business and E-Government - ICEEG '18*, 2018, pp. 79–83. doi: 10.1145/3234781.3234792.

[15] L. J. P. Doce and M. R. D. Ching, "RA 10173 and its challenges to Philippine state universities and colleges' compliance performance," in *Proceedings of the 2nd International Conference on E-commerce, E-Business and E-Government - ICEEG '18*, 2018, pp. 69–73. doi: 10.1145/3234781.3234789.

[16] M. P. Canares, "Opening the local: full disclosure policy and its impact on local governments in the Philippines," in *Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance*, Oct. 2014, pp. 89–98. doi: 10.1145/2691195.2691214.

[17] J. v. Presbitero and M. R. D. Ching, "Assessing compliance of Philippine state universities to the data privacy act of 2012," in *Proceedings of the 2nd International Conference on E-commerce, E-Business and E-Government - ICEEG '18*, 2018, pp. 90–94. doi: 10.1145/3234781.3234800.

[18] R. J. C. Tanate-Lazo and D. C. Cabonero, "Philippine Data Privacy Law: Is it Implemented in a Private University Library, or Not?," *Library Philosophy and Practice*, 2021.

[19] L. J. P. Doce and M. R. D. Ching, "RA 10173 and its challenges to Philippine state universities and colleges' compliance performance," in *Proceedings of the 2nd International Conference on E-commerce, E-Business and E-Government - ICEEG '18*, 2018, pp. 69–73. doi: 10.1145/3234781.3234789.

[20] R. T. G. Flores and M. R. D. Ching, "Philippine SUCs compliance performance on RA 10173," in *Proceedings of the 2nd International Conference on E-commerce, E-Business and E-Government - ICEEG '18*, 2018, pp. 74–78. doi: 10.1145/3234781.3234790.