# DATA PRIVACY BEST PRACTICES OF A LOCAL HIGHER EDUCATIONAL INSTITUTION: A MODEL FOR GOVERNANCE

**RUSHID JAY S. SANCON**
rushidjay.sancon@lspu.edu.ph
Laguna State Polytechnic University
Philippine Christian University
Philippines

**DOI: https://doi.org/10.54476/ioer-imrj/688585**

## ABSTRACT

*The passage of the Data Privacy Act of 2012, establishes a new data privacy framework for all industries and sectors, whether in public or private. Different agencies' policies have aimed to foster innovation and the development of commercial and public sector technical skills. The hit COVID-19 pandemic pushed academic institutions for a paradigm shift in the delivery of instructional and administrative services in online platforms. This study assessed the Laguna State Polytechnic University's (LSPU) data privacy policies and governance transformation to determine its best practices and establish an informational privacy framework. LSPU commenced its full compliance in 2017, hence the researcher chose the respondents whose employment at the university is between 2017 and 2021 to ensure they have sufficient experience and skill in the implementation of the Data Privacy law promulgated in 2012 and its rules and regulation in the university. Questionnaires were utilized to collect information, and interviews with unit heads and university staff validated the results. Based on the study's hypothesis, it is determined that the governance of existing data privacy policies at the institution is completely established. Since the results of the analysis revealed a significant correlation, the respondents strongly support a very high degree of data privacy implementation oversight. Further, using the path-analysis technique, it was found that the governance has a positive effect on the current practices of data privacy in the university. Finally, the study revealed that when there is a certain policy change responsive to the data privacy law that is to be implemented in the university, it is expected that practices in the implementation of data privacy law will show significant change.*

*Keywords: Data Governance, Data Practices, Informational Governance, Data Privacy Model*

## INTRODUCTION

Privacy is an essential component of democratic processes. It has a universal value that is beyond an individual's real but one that concerns the whole society.

The protection accorded by the constitution on privacy rights is critical not just for individual rights but also for democracy: it safeguards the integrity of the communication infrastructures that underlie democratic self-autonomy. However, the privacy argument sometimes lacks the definition of privacy and overlooks its public worth (Seubert & Becker, 2021).

With the passage of the Data Privacy Act of 2012, it establishes a new data privacy framework for all industries and sectors, whether in public or private. The new data privacy law mandates compliance with the five pillars of data protection. The same shall be investigated in the privacy governance of the Laguna State Polytechnic University - System to develop an effective informational privacy governance

framework suitable to the organizational practices and processes of the university.

The COVID-19 pandemic pushed academic institutions for a paradigm shift in the delivery of instructional and administrative services in online platforms. Those in tertiary education, have shifted from traditional face-to-face classes to flexible learning. This is not only applicable in the delivery of instruction but also applied in providing services from student enlistment, pre-enrolment process, assessment of fees, and payment. The need for compliance of academic institutions on data privacy protection becomes more demanding and relevant at this time. Assessing the same would give the institution evidenced-based reference in designing data privacy plans, strategies, and mechanisms that will suit the organizational dynamics and culture of the academic institutions.

It may be relevant to note however that the use of online platforms and channels in educational institution's workplace have generated big amount of data from people. The determination of data privacy measures and behavior/values towards the protection of the same within the institution would be a benchmark in establishing a framework ideal for the school's organization.

During the pandemic, information and data management are critical considerations. According to Malindog-Uy (2020) the challenges of internet security and privacy in the Philippines as a result of the growth of online and distance learning. The problem of data privacy has been largely ignored in this context since the majority of attention has been focused on developing new teaching modes. The exposure of learners to the digital world raises their risk of data leaks, identity theft, and other types of data breaches (Estrellado, 2021).

The researcher explores the data privacy practices of one tertiary education about its data privacy governance.

## OBJECTIVES OF THE STUDY

This study assessed the Changes of Data Privacy Practices and the Governance Change in the informational privacy model in the Laguna State Polytechnic University.

Specifically, this study aims to answer the following questions:

1. Determine the level of Governance of Current Data Privacy Practices in the Four Campuses of the Laguna State Polytechnic University in terms of:
    1.1 Organizational Commitment;
    1.2 Employee Privacy Accountability;
    1.3 Data Risk Assessment;
    1.4 Data Risk Control; and
    1.5 Informational Recovery.
2. Identify the level of Current Practices on Data Privacy Law implementation among administrative and academic units, and their respective personnel in the four regular campuses of the Laguna State Polytechnic University in terms of:
    2.1 Data Privacy Governance Planning;
    2.2 Data Collection Practices;
    2.3 Data Control Operations;
    2.4 Assessment of Data Privacy Risk; and
    2.5 Security Incident Management.

3. Measure the effects of the Governance of the Current Data Privacy Practices on the Current of Practices on Data Privacy Act implementation among academic units and administrative units in the four campuses of the Laguna State Polytechnic University.

4. Evaluate the Informational Privacy Governance Model that should be implemented in the Laguna State Polytechnic University System.

## METHODOLOGY

In this study, a descriptive method of research was employed to determine and interpret the meaning and significance of changes in data privacy practices toward the development of data privacy governance from 2017 to 2021, as perceived by the respondents. Quantitative research was utilized to measure the extent of this

issue, using numerical values to identify the size of objects or the relationship between independent and dependent variables (Trinidad, 2018).

The study surveyed Laguna State Polytechnic University's internal Data Users and implementors, including Academic Unit Heads (Deans and Associate Deans), Administrative Unit Heads (Directors and Chairpersons), and non-teaching personnel from the four regular campuses, which totals 323 respondents. Their experience, knowledge, and engagement with informational privacy governance serve as a valid and reliable measure of the changes to data privacy practices and governance.

Before beginning the research, the researcher sent letters requesting permission from the University President, Vice-Presidents, and Campus Directors. An orientation was held either in-person or via Zoom or online conference to explain the objectives and directions for completing the questionnaire. Informal interviews were conducted for further clarification if needed. The questionnaires were distributed both physically and online, with assistance from the ICTS Office of LSPU-Siniloan Campus for the online distribution. After collecting the data, it was monitored and prepared for analysis and statistical treatment. To ensure confidentiality, a confidentiality agreement and consent form was included with the physical questionnaires and online forms.

This study utilized a survey questionnaire as the main instrument to focus on data privacy practices and the culture of data privacy governance. A thorough review of related literature and studies was conducted to ensure that the questions posed would be based on a solid foundation. The questionnaire was then checked by an advisor and a panel of experts, followed by a pilot test for validation and reliability.

The researcher used the mean and standard deviation as statistical tools in the study. Correlation analysis was utilized in the study to determine the significant relationship between two or more variables. In particular, Spearman's rank-order correlation (Spearman's rho) was used. Spearman's rho is applicable when determining the relationship of at least two ordinal data (ranked data) or parametric data that fall short on the normality test.

**Table 1**
*Likert-type Scale and its Verbal Interpretation*

| Likert-type of Scale | Verbal Interpretation |
|---|---|
| 4 – strongly agree | Very High |
| 3 – Agree | High |
| 2 – Disagree | Low |
| 1 – Strongly disagree | Very Low |

## RESULTS AND DISCUSSION

### 1. Governance of Current Data Privacy Practices

**Table 2**
*Level of Governance of Informational Privacy*

| Indicators | Weighted Mean | Std Dev | Verbal Interpretation |
|---|---|---|---|
| Organizational Commitment | 3.607 | 0.497 | Very High |
| Employee Privacy Accountability | 3.678 | 0.446 | Very High |
| Data Risk Assessment | 3.706 | 0.580 | Very High |
| Data Risk Control | 3.707 | 0.518 | Very High |
| Informational Recovery | 3.552 | 0.527 | Very High |
| **Over - All Mean** | 3.650 | 0.514 | Very High |

Table 2 provides a very high level of governance on informational privacy with an overall mean of (M=3.650, SD=0,541). The data would reveal that Data Risks Control got the highest mean of (M=3.707, SD=0.518). Also, there is a very high level of governance changes in terms of Data Risk Assessment mean of (M=3.706, SD=0.580). Also, Employee Privacy Accountability got a very high level of change with a mean of (M=3.678, SD=0.446). Followed by Organizational Commitment it got a very high level with a mean of (M=3.607, SD=0.497). Although, still on a very high level, Informational Recovery got the lowest mean of (M=3.552, SD=0.527).

Recent legislative efforts to rein in contractual flexibility recognize this vulnerability but are incapable of resolving it on their own—and neither can data ownership. The latter is both improbable and insufficient as a solution to the

issues at hand (Delacroix & Lawrence, 2019). Clients struggle to regain control over their data as a result of rising technical complexity and varied data-exploitation corporate tactics. However, it looks as if data protection legislation makes certain assumptions about human decision-making to strengthen individual control (Van Ooijen & Vrabec, 2019).

The survey respondents reported a very high level of organizational commitment to data privacy practices and security measures. They had a strong sense of value towards the data privacy practices implemented, developed security measures for the organization, and developed security-focused data privacy response practices in their day-to-day operations. The respondents also observed the governance change in developing best practices based on international and domestic standards for data protection. The organization also developed ways to communicate the results of the Privacy Impact Assessment. The lowest indicator among the survey questions was the "participatory planning scheme" with a mean of 3.365. Likewise, organizational Commitment, which is the fundamental link in the information security chain, is a significant predictor of employees' ISP acceptance behavior. Managers should make additional efforts to strengthen employees' sense of identification and belongingness with their organizations. Due to the fact that high-commitment workers are internally motivated to safeguard their businesses' information assets, managers may encourage them to assist others in performing security behaviors (Liu et al., 2020). Findings of the study show that the management of the university includes data privacy as an integral part of the operations which is also in need of proper monitoring if properly implemented and observed.

The respondents also rated that the employees have a very high level of Governance of Changes on Informational Privacy in terms of Employee Privacy Accountability. This was reflected in their adherence to data privacy principles such as transparency, proportionality, legitimacy of purpose, knowledge of legal consequences of data breaches, and providing immediate remedial action for unauthorized/malicious disclosures. Furthermore, the respondents perceived the employees to have a sense of accountability when it comes to upholding the rights of data subjects. The lowest mean was for integrating remedial actions in addressing risks, but it was still very high at M=3.409. Employees and managers may disagree with the degree to which employers seek confirmation in data rather than from employees themselves, thereby increasing employee-focused collection of data, but in the process of technological advancement rather than employee participation, and fostering the continuous measurement of human resources practices (Jeske and Calvard, 2020). Employees have high regard for the proper treatment of data which is manifested by their very high extent of sense of accountability, integrating remedial actions, and adherence to data privacy principles.

The results of this study show that respondents perceive a very high level of governance of changes in informational privacy in terms of data risk assessment. This is evidenced by a mean of 3.706 (SD=0.580) and includes developing regular assessment and evaluation of system security measures (M=3.728, SD=0.671), developing risk mitigation plans (M=3.728, SD=0.600), updating Privacy Impact Assessment reports (M=3.721, SD=0.613), developing instruments for data risk assessment (M=3.709, SD=0.612), measuring vulnerability to risk (M=3.700, SD=0.625), conducting data risk assessment in Privacy Impact Assessment (M=3.700, SD=0645), training administrative units in self-assessing risks (M=3.697, SD=0.626), and preparing and submitting reports to the Data Privacy Officer (M=3.684, SD=0.649). While the institutions “Developed a mechanism that administrative offices conduct privacy risks are done periodically” observed by the respondents to be very high level with a mean of (M=3.675, SD=0.671) but it got the lowest mean among the indicators. The institution, like many organizations, big data has developed into a valuable asset, offering enhanced operations. Results indicate that the university provides support to its employees on how to cascade information about data risk assessment through training and providing a system, together with mechanisms, and guidelines. The university ensures that employees are

equipped with the necessary competencies on how to construct plans to address risk.

The respondents revealed that there is a very high level of governance change in terms of data risk control and informational privacy. This included developing policies to ensure data collection from individuals, having a system that informs the data subject of the purpose of collection, developing policies that are compliant with the Data Privacy Act of 2012, having a system that requires the collection of data for specified purposes, implementing mechanisms that ensure the data subject is informed and aware of the extent of data collection, and developing policies to anonymize and de-identify information of data subjects. The lowest level of mean was for developing a system that ensures to the data subject that the information being collected is necessary for the program. Employees' security practices on data risk control are critical for the comprehensive protection of an organization's information (Herath et al., 2018). People are key in these systems; therefore, data governance should give incentives and consequences to encourage good behavior. Data governance requires cooperation between organizations and individuals (Janssen et al., 2020). This shows that the university has a procedure in data processing and release which is progressing in terms of its implementation.

The respondents reported a very high level of governance when it comes to mitigating data breaches and protecting the data of data subjects. This includes the development of systems, training of administrative units, implementation of the institution's data recovery procedures, development of physical security measures, and technical security measures, as well as regular policy development/updates and security policy implementation. Dissemination of the data privacy management information also had a very high level, though developing treatment on security measures that immediately address the data privacy issues of data subjects had the lowest mean among the indicators. This is supported by Greve et. al. (2020). While this is unquestionably a beneficial development in terms of reducing digital inequality, the rapid use of internet-connected equipment has resulted in greater security concerns.

Data recovery plays a significant role in the processing of data. Based on the results, the university has a very high extent of changes of governance. This reveals that there has been a policy implemented in the university concerning the handling of data or information. This can be attributed to the initiatives of the university in digitizing its processes.

## 2. Current of Practices on Data Privacy Law

**Table 3**

*Level of Practices on Data Privacy Law Implementation*

| Indicators | Weighted Mean | Std Dev | Verbal Interpretation |
|---|---|---|---|
| Data Privacy Governance Planning | 3.324 | 0.463 | Very High |
| Data Collection Practices | 3.646 | 0.386 | Very High |
| Data Control Operations | 3.730 | 0.489 | Very High |
| Assessment of Data Privacy Risk | 3.678 | 0.559 | Very High |
| Security Incident Management | 3.729 | 0.550 | Very High |
| **Over - All Mean** | 3.621 | 0.489 | Very High |

Table 3 shows the Summary of the Level of Practices in Data Privacy Law Implementation. All indicators got a very high level of practice with a mean of (M=3.621, SD=0.489). The data presented shows that Data Control Operations got the highest mean of (M=3.730, SD=0.489). Followed by Security Incident Management with a mean of (M=3.729, SD=0.550), then by Assessment of Data Privacy Risk with a mean (M=3.678, SD=0.559). It also revealed that among the five indicators, Data Collection Practices come at fourth with a mean (3.646, SD=0.386). Lastly, the lowest among the indicators is Data Privacy Governance Planning with a mean of (M=3.324, SD=0.463).

The institution is observed to have a very high level in terms of providing a schedule for regular compliance assessments and security

audits, allowing the participation of stakeholders in Privacy Governance planning, considering best practices in the domestic security standards on planning, consideration of technological advancement, and evaluation of the Privacy Management Plan. It is also observed to have a high level of change in terms of considering practices in the international security standards and gathering inputs through surveys or interviews on the data privacy practices for data governance planning. The lowest mean among the indicators is observed to be “Organizational Data Policy Planning are participated by stakeholders (Students/ Faculty/ Non-teaching Staff)” which still has a high mean of 3.180. This is essential considering that regulatory pressure has been growing in recent years for a number of reasons, and it is becoming more costly on the institution’s budgetary requirements. Management needs a regulatory framework, through extensive and careful planning and strategizing of organizational course of action, that reassures members of the institution, supports the adoption of a uniform security architecture, and dispels the anxieties of engineers in charge of technical controls. Based on the results, the university has initiatives on integrating data privacy in the development of its strategic directions which is participatory in nature as evident in the formulation of milestones set in the strategic plans and objectives.

The institution has a very high level of practice on Data Privacy Law Implementation in terms of Data Collection Practices. The highest mean was for the collection of sensitive data being authorized by law or the implementing rules. Other practices which received a very high level of response were the collection of personal data being based on the Data Privacy Act and its implementing rules, programs of the university is based on its designed purpose, data subjects being made aware of the purpose of collection, extent of the collection, and the policy relative to the withdrawal of their consent in processing of information, collection of personal data not being against morals, anonymization and de-identification of collected information from data subject, and informing data subjects on the legitimacy of collection. The act of collecting data coming directly from an individual or the data subject received the lowest mean. These findings find support in the discussion of Serzo (2020) where he stated that data privacy and protection have reached the top of the list of concerns that organizations in the Philippines, particularly digital platforms, are concerned about following the passage of the Philippine Data Privacy Act of 2012 (the "DPA") and the National Privacy Commission's (NPC) aggressive enforcement efforts. The fact that the DPA is classified as legislation with a three-fold accountability, which forbids the improper treatment of personal data, may contribute to the law's widespread acceptance. Results of the study show that in the university, the security of data is treated with a high extent of priority.

This survey reveals that the institutions have undergone a very high level of changes in terms of data control operations and data privacy law implementations. The highest mean of 3.827 was observed for the practice of proper documentation of authorized disclosure of the data freely given by a data subject. Other areas of high change include policies introduced to ensure that the personal data will only be used for declared purposes, agreement or contract review to ensure data privacy policy compliance, employment of steps to protect sensitive data loss, personal data loss, and personal data access, the introduction of inventory processes system for data and policies concerning the restoration of data in case of loss. The lowest mean of 3.446 was observed for the employment of reasonable steps to protect sensitive data access, yet still, this area saw a very high level of change. This finds support in the study of Gonzales and Ching (2018) which provides that there are links between data collection, dissemination, technology, privacy classification about public expectation, and the political and legal considerations that surround them.

The respondents observed a high level of in terms of assessment of data risks and compliance with the National Privacy Commission's Privacy Risk Management. Moreover, the respondents had a very high level of change in the training of employees for self-assessment of risks in their respective units as well as the regularity of its occurrence during the Privacy Impact Assessment and the vulnerability to risk in the data management. Lastly, the regular assessment of

data privacy risks of the institution got the lowest level of mean. Considering that LSPU has institutionalized the online processing of services either in the area of academics or administration, the processing of data has been more efficient but exposed to additional risks. With the nature of cyber technology, which serves as an innovative medium of expression for students and provides access to international information, comes the emergence of new challenges. Students' improved access to the internet on university campuses has increased cyber piracy and other forms of unethical cyber conduct (Aderibigbe and Ocholla, 2020).

The survey found that respondents had a very high level of data privacy practices in terms of security incident management. This included updating security policies with respect to the processing of data, making units aware of security measures in handling unauthorized disclosures, integrating data privacy policies into day-to-day operations, and disseminating policies on managing information risk. The findings are in line with the discussion of Richardson et. al. (2020) citing Zammani & Razali (2016). Their study explained that investigating patterns, learning from worst-case situations, and adapting to the changing environment are the most effective ways to safeguard a school on the internet. Taking those risky actions and taking meaningful action is an important element of the governance change process. As revealed by the results, the university ensures that the existing policies and regulations are implemented to a high extent by providing support to its employees on how to be informed and make necessary measures on how to internalize these data privacy-related policies and regulations.

### 3. Normality of the Distribution

Since we have a sample size of 323, determining the distribution of the two variables is important in choosing an appropriate statistical tool or method. So a Shapiro – Wilk (W) test was performed and showed that the distribution of the practices on Data Privacy Law Implementation, W(323) = 0.690 ;p–value = 0.000 and Governance of Changes on Informational Privacy, W(323) = 0.718;p–value = 0.000. Since thep–value is less than 0.05 then we can say that the distribution deviates from normality or is not normally distributed. Based on this outcome Spearman's rho correlation a non – parametric test was used to determine if there is a significant relationship or effect between the two variables.

**Table 4**
*Tests of Normality of the Distribution*

| | Shapiro-Wilk | | |
|---|---|---|---|
| | Statistic | Df | Sig. |
| Level of Changes of Practices on Data Privacy Law Implementation | .690 | 323 | .000 |
| Level of Governance of Changes on Informational Privacy | .718 | 323 | .000 |

Since we have a sample size of 323, determining the distribution of the two variables is important in choosing an appropriate statistical tool or method. So a Shapiro – Wilk (W) test was performed and showed that the distribution of the practices on Data Privacy Law Implementation, W(323) = 0.690 ; p–value = 0.000 and Governance of Changes on Informational Privacy, W(323) = 0.718;p–value = 0.000. Since the p–value is less than 0.05 then we can say that the distribution deviates from normality or is not normally distributed. Based on this outcome Spearman's rho correlation a non – parametric test was used to determine if there is a significant relationship or effect between the two variables.

### 4. Changes Practices on Data Privacy Law Implementation and Governance of Informational Privacy

Spearman's rho correlation is a non-parametric test used to determine whether there is a relationship or influence between the Practices of Data Privacy Law Implementation and Governance of Informational Privacy in the Four Campuses of The Laguna State Polytechnic. Table 14 shows that there is a high positive correlation between Changes in Practices on Data Privacy Law Implementation and Governance of Changes in Informational Privacy (rho = 0.698). Thep–value = 0.000, N= 323 generated from the table explains that we have enough evidence to show that

Changes in Practices on Data Privacy Law Implementation were significantly influenced by Changes of Governance on Informational Privacy.

**Table 5**
*Correlation Analysis on Practices on Data Privacy Law Implementation and Governance of Change on Informational Privacy*

| | | | Level of Practices on Data Privacy Law Implementation | Level of Governance on Informational Privacy |
|---|---|---|---|---|
| Spearman's rho | Level of Changes of Practices on Data Privacy Law Implementation | Correlation Coefficient | 1.000 | .698** |
| | | Sig. (2-tailed) | | .000 |
| | | N | 323 | 323 |
| | Level of Governance of Changes on Informational Privacy | Correlation Coefficient | .698** | 1.000 |
| | | Sig. (2-tailed) | .000 | |
| | | N | 323 | 323 |

Changing policy texts and concepts can prompt and allow school systems to engage in educational system building—that is, (re)building educational infrastructures to support more coherent visions for instruction, albeit in a few school subjects (Spillane et al., 2019). The widespread adoption and implementation of digital technologies by organizations has resulted in a massive transformation that has the potential to impact the internal operations and processes of many organizations. This transformation has an effect on various levels and stages of output creation and services in an organization, ultimately resulting in changes to their organizational structures and practices (Kretschmer & Khashabi, 2020).

Based on the result of the study, the changes in the governance and the changes in the practices on implementing the data privacy law are positively correlated in the context of the Laguna State Polytechnic University. All indicators of governance (organization commitment, employee privacy accountability, data risk assessment, data risk control, and informational recovery) and practices (data privacy governance planning, data collection practices, data control operations, assessment of data privacy risk, and security incident management) are both very high. Thus, when there is a certain change in policy responsive to the data privacy law that is to be implemented in the university, it is expected that practices in the implementation of data privacy law will show significant change.

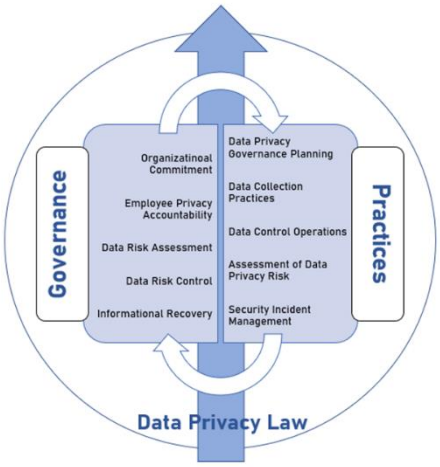


*Figure 1. Informational Privacy Governance Framework for Laguna State Polytechnic University System*

## CONCLUSIONS

It is concluded that changes in the level of governance on informational privacy led to changes in the implementation practices of data privacy law in the university. Since the outcome of the analyses found a positive relationship, a very high level of change in the governance results in a very high level of change in the implementation practices.

In view of the findings and conclusion, the following are recommended: Sustain and develop additional measures to ensure Data Control Operations practices are in place in the implementation of policies. Data Privacy Governance Planning, although still has a very high level of change, the same may still be improved by being more inclusive by allowing other stakeholders (regulatory agencies like CHED, National Privacy Commission, and accrediting bodies like AACCUP) to participate and be heard in the data privacy governance planning. Also, since the high extent of changes in governance might result in changes in the implementation practices of data privacy law, it is recommended that policies or other similar initiatives to strengthen the level of adherence to data privacy law should be disseminated in a wider range to ensure its success. Establish defense protocols against data breaches and malicious disclosures and inclusion of Data Protection Strategic Initiatives in the Institution's Strategic Plan which will set the informational privacy goals and

objectives of the institution. With this, priorities and actions will be institutionalized.

## RECOMMENDATIONS

Data Risks Control practices may be sustained and be considered to be improved over time to be more adaptive in the present and future rules and regulations, organizational environment, technological advancement, and infrastructure development. Informational Recovery by the university may be improved by consulting experts in developing treatment on security measures that immediately address the data privacy issues of data subjects, whether internal or external.

The institution should sustain and develop additional measures to ensure Data Control Operations practices are in place in the implementation of policies. On one hand, Data Privacy Governance Planning, although still has a very high level of change, the same may still be improved by being more inclusive by allowing other stakeholders (regulatory agencies like the Commission on Higher Education (CHED), National Privacy Commission (NPC), and accrediting body like AACCUP) to participate and be heard in the data privacy governance planning.

Changes in governance might result to changes in the implementation practices of data privacy law, it is recommended that policies or other similar initiatives to strengthen the level of adherence to data privacy law should be regularly disseminated in a wider range to ensure its success.

Inclusion of Data Protection strategic initiatives in the Institution's Strategic Plan which will set the informational privacy goals and objectives of the institution. By doing so, priorities and actions will be institutionalized in the university's governance framework. For future research, external stakeholders' input may be considered, and those in the teaching faculty be included to assess the processes and practices when it comes to processing personal and sensitive information of students, being the primary clientele of the institution.

## REFERENCES


Aderibigbe, N. A., & Ocholla, D. N. (2020). Insight into ethical cyber behaviour of undergraduate students at selected African universities. *South African Journal of Information Management, 22*(1), 1-8. http://dx.doi.org/10.4102/sajim.v22i1.1131

Delacroix, S., & Lawrence, N. D. (2019). Bottom-up data trusts: disturbing the 'one size fits all'approach to data governance. *International Data Privacy Law, 9*(4), 236-252. https://doi.org/10.1093/idpl/ipz014

Estrellado, C. J. (2021). Transition to post-pandemic education in the Philippines: Unfolding Insights. *International Journal of Scientific and Research Publications, 11*(12). https://doi.org/10.29322/IJSRP.11.12.2021.p12074

Gonzales, E. C., & Ching, M. R. D. (2018). Performance compliance of Philippine national government agency on the data privacy act of 2012: a qualitative case study. *In Proceedings of the 2nd International Conference on E-commerce, E-Business and E-Government* (pp. 79-83). https://doi.org/10.1145/3234781.3234792

Greve, M., Masuch, K., Hengstler, S., & Trang, S. (2020). Overcoming digital challenges: A Cross-Cultural Experimental Investigation of Recovering from Data Breaches. In ICIS. bit.ly/3p4OJUT

Herath, T., Yim, M. S., D'Arcy, J., Nam, K., & Rao, H. R. (2018). Examining employee security violations: moral disengagement and its environmental influences. *Information Technology & People, Vol. 31* No. 6, pp. 1135-1162. https://doi.org/10.1108/ITP-10-2017-0322

Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. *Government Information Quarterly, 37*(3), 101493. https://doi.org/10.1016/j.giq.2020.101493

Jeske, D., & Calvard, T. (2020). Big data: lessons for employers and employees. *Employee Relations: The International Journal, Vol. 42* No. 1, pp. 248-261. https://doi.org/10.1108/ER-06-2018-0159

Kretschmer, T., & Khashabi, P. (2020). Digital Transformation and organization design: an integrated approach. *California Management*

*Review,* *62*(4), 86–104. https://doi.org/10.1177/0008125620940296

Liu, C., Wang, N., & Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management,* *54*, 102152. https://doi.org/10.1016/j.ijinfomgt.2020.102152

Malindog-Uy, A.R. (2020). "Blended learning" in virus-hit Philippines. The ASEAN Post. https://theaseanpost.com/article/blended-learning-virus-hit-philippines

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for Cyber security in schools: The Human Factor. *Educational Planning*, *27*(2), 23- 39. https://eric.ed.gov/?id=EJ1252710

Serzo, A. L. O. (2020). Cross-border data regulation for digital platforms: data privacy and security. Philippine Institute for Development Studies (PIDS). http://hdl.handle.net/10419/241036

Seubert, S., & Becker, C. (2021). The democratic impact of strengthening European fundamental rights in the digital age: The example of privacy protection. *German Law Journal, 22*(1), 31-44. https://doi.org/10.1017/glj.2020.101

Spillane, J. P., Seelig, J. L., Blaushild, N. L., Cohen, D. K., & Peurach, D. J. (2019). Educational System Building in a Changing Educational Sector: Environment, Organization, and the Technical Core. *Educational Policy, 33*(6), 846–881. https://doi.org/10.1177/0895904819866269

Trinidad, J. E. (2018) Researching Philippine realities: A Guide to qualitative, quantitative, and humanities research. bluebooks. Ateneo De Manila University Press.

Van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of Consumer Policy,* *42*(1), 91-107. https://doi.org/10.1007/s10603-018-9399-7

## AUTHOR'S PROFILE

**Atty. Rushid Jay S. Sancon** is an Associate Professor III, and presently the Campus Director of Laguna State Polytechnic University (LSPU) – Siniloan campus since January 2022. Prior to his designation as Campus Director, he occupied various positions in the LSPU.

As to his educational credentials, he graduated Doctor of Philosophy in Development Administration major in Public Governance at the Philippine Christian University. He also earned his Master of Laws (LLM) degree at San Sebastian College Recoletos-Manila. He finished his Juris Doctor from Laguna State Polytechnic University, and his Bachelor of Arts major in Economics at the Cagayan State University-Gonzaga Campus.

## COPYRIGHTS