Beyond compliance: Analysis of data privacy implementation

Justfer John D. Aguilar

College of Education, Arts and Sciences, University of Southern Mindanao-Kidapawan Campus, Philippines

JOMEINO
ISSN:
2522-381X (Print)
2521-7054 (Online)
DOI: 10.31039/jomeino

Received 12 December 2023
Revised 20 January 2024
Accepted 25 January 2024

Citation: Aguilar, J. J. D. (2024). Beyond compliance: Analysis of data privacy implementation. *Journal of Management, Economics, and Industrial Organization, 8*(2), 78-93. http://doi.org/10.31039/jomeino.2024.8.1.4

corresponding author:
jjdaguilar@usm.edu.ph

Abstract

This study was conducted to assess the level of implementation of data privacy as perceived by Human Resource Management Officers (HRMO). This study employed a descriptive research design, in which the researcher collected quantitative data through survey questionnaire employing random sampling procedure to the 100 members of the Council of Human Resource Management Officers (CHRMP) of North Cotabato. Findings of the study revealed that data protection policies obtained the highest weighted mean with a qualitative description of very highly implemented which implies that organization ensures an enabling policy pursuant to the provision of RA 10173 or Data Privacy Act of 2012. However, study also revealed that right to damages emerge with the lowest weighted mean equivalent to moderately implemented. This denotes that there were existing limitations in the organization in properly addressing issues relevant to data breaches. Notably, lack of awareness in DPA, lack of appropriate resources, complex regulatory landscape, emerging technologies and DPO appointment were identified as challenges in the implementation. Moreover, further research is recommended to ascertain a comprehensive understanding on the challenges faced by the human resource management officers in the data privacy implementation.

Keywords: *Data Privacy, implementation, human resource management officers*

JEL Classification Codes: J18, J28, L52, O15, Y80, Z18

1. Introduction

In the advent of digital information revolution, data is considered as one of the most important resources in any organization. Proper handling and safekeeping of this asset entails organization to provide mechanism to safeguard individuals right and privacy. This is the assertion of Chandrasekeran et al. (2023) that the rapid changing landscape necessitates proper managing, storing, and retrieving of crucial records of the employees. Thus, subjected human resource management's crucial role in dealing with data security. Human resource management ensures individual data security of the workplace. This office of the organization works with personal data of employee's day after day. In fact, human resource hold records starting from the employees first day until his or her retirement. Apart from that, they hold relevant information that are considered highly confidential in nature. This is also the assertion that human resource management is compelled to secure the data of all its employees involving cybersecurity and other data threats. Many organizations had adopted HR analytics in their processes however it poses threats to their information making the human resource management a very crucial entity in preventing pilferage (Jha, 2022).

In the Philippines, mechanism to ensure data security was established through Republic Act No. 10173 of the Philippines, also known as "Data Privacy Act of 2012" mandating public and private organizations, agencies, and institutions to protect and safeguard sensitive and confidential data of its members. Thus, provide a nuance to monitor compliance to data protection and privacy. However, Pitogo (2019) revealed that there are other government agencies that are not compliant with the Data Privacy Act of 2012. He identified several factors such as attitude, awareness, and resources towards this non-compliance. This depicts the pivotal role that human resource professionals play in any organization. As such, they have the responsibility to ensure that organization is compliant despite the changing conditions of the human resources (Wijesingha & Wickremeratne, 2020). A similar assertion of Pooja and Greeshma (2022) proves the important role that human resource practitioners play in handling and securing employees data.

The researcher argues that human resource practitioners were faced with challenges in implementing data privacy and security in their respective units. As the organization embraces advancement and integration of ICT in the core processes, this poses formidable challenges in securing the implementation of the law and ensuring protection of all its employee. As such, this research sought to answer the following objectives:

1. *Determine the perceived level of implementation of data privacy act among human resource management officers.*
2. *Identify the challenges faced by human resource management officers in the implementation of data privacy.*

2. Literature Review

2.1. Data privacy and its implementation

The rapid advancement of technology compelled organizations to safeguard the data of its members. The capabilities and networks of technological advancement threaten the security of data and personal information, hence, a need to have data privacy. Data privacy is any mechanism used to protect the people from the current prevailing threats of digital age (Foronda et al., 2023). Gonzales and Ching (2018) asserted that data privacy are measures to ensure privacy protection from any forms of accessibility and data breaches. As mentioned by Alafaa (2022), the concept of data privacy stems from the assertion of fundamental human rights that are essential to forming a free society. This is a right of an individual to ensure that relevant personal information will not be accessed by unauthorized parties.

Consequently, Alafaa (2022) noted that data protection is the primordial responsibility of any organization. Several organizations implemented the provision of the General Data Protection Regulation (GDPR). This is a mechanism that recently harmonized to protect the confidential data of its people from various breaches (Machado et al., 2023). Savić and Veinović (2018) said that GDPR provides a comprehensive framework in managing sensitive data and protocols for organizations in collecting and processing data. Additionally, this framework has been influential in the birth of other relevant laws and data regulations across the world. In the Philippines, data privacy implementation has been crucial. In fact, National Privacy Commission was established following the enactment of Republict Act No. 10173 or the Data Privacy Act of 2012 (Ching et al., 2018). The implementation of the law stems from the purpose of ensuring that human rights will be protected from all forms of threat (Foronda et al., 2023).

2.2. Challenges in the implementation of data privacy

Several research noted that lack of awareness and understanding challenges the implementation of any regulation and laws (Chua et al., 2017; Pitogo, 2019). This challenge often stems from various factors such as insufficient dissemination of information, complex legal language, and inadequate educational programs. Foronda et al (2023) noted that without proper comprehension of regulations and laws, individuals and organizations may inadvertently violate them or struggle to adhere to compliance requirements. Addressing this issue requires targeted efforts to enhance public awareness, provide accessible educational resources, and simplify legal frameworks to promote better understanding and compliance.

Considerably, the failure to adhere to legal provisions often arises from organizations lacking dedicated data privacy officers. The pivotal role of a Data Protection Officer (DPO) in ensuring compliance with data protection regulations has been underscored by Kupny (2019) and Nerka (2017). The DPO's responsibilities encompass providing expert guidance, overseeing compliance, and ensuring adherence to data processing regulations (Kupny, 2019). This multifaceted role demands a diverse skill set, spanning legal, managerial, and cybersecurity domains, to effectively navigate sociotechnical risks (Ciclosi & Massacci, 2023). Additionally, the appointment of a DPO can signal an organization's commitment to corporate social responsibility (Nerka, 2017). Warren (2002) further highlights the critical role of a Privacy Officer within the healthcare sector, particularly in achieving and maintaining compliance with privacy regulations.

The complexity of data privacy regulation, with its international, regulatory and statutory provision, poses a significant challenge to its effective implementation (Busch, 2011). This is further complicated by the rapid evolution of data analytics and the lack of uniformity in privacy definitions globally (Jaiswal, 2020). Weber ad Staiger (2017) asserted that difficulty in achieving digital privacy in the online world adds to this challenge. Despite these obstacles, companies can mitigate the risk of data privacy breaches through effective user access restrictions (Haller, 2012).

Furthermore, the rapid advancement of technology has significantly impacted data privacy implementation. Weber (2015) highlights the emergence of advanced data security and privacy measures, such as the privacy-preserving Apriori algorithm and differential privacy. However, these measures are being challenged by the use of new technologies, which facilitate the collection, storage, and processing of personal data (Friedewald et al., 2010). Mohan Rao P et al. (2021) asserted that people are living in a data driven world where personal data had been generated in almost every form of public domain. The broad utilization of internet posits vulnerable threats to data security. The proliferation of usage of social media, smartphone applications and internet commerce could directly harm confidential data and so with the implementation of data privacy.

3. Methodology

The research design utilized in this study was descriptive research. Descriptive research is a methodological approach used to describe observable patterns of behavior and a way to obtain a general overview of the variables. Calmorin and Calmorin (2012) defines this as a method that provides essential knowledge to measure all types of data in quantitative research. The respondents of the study were the 100 members of the Council of Human Resource Management Officers of North Cotabato (CHRMP) selected through random sampling.

Before the conduct of the research, the researcher secured permission from the President of the organization. After obtaining permission, the researcher conducted the study. The researcher made use of a survey instrument adopted from Castro (2021) using google forms and it was distributed to potential respondents via email, accompanied by details about the survey's objective and how the collected data would be used. This study utilized descriptive statistics. Mean and percentages were used to analyze the data of the respondent's perceived level of implementation of data privacy. On the other hand, frequency count and percentages were used to quantify the challenges in the implementation of data privacy.

4. Results and discussions

As shown in Table 1, the overall mean for the level of implementation is *3.56* with a qualitative description of *highly implemented*. This implies that they possessed a comprehensive understanding of the data privacy act, as mandated by the law. The data likewise denote that human resource professionals are well-equipped to implement the guidelines of data privacy act in their processes.

Moreover, item 2 "*Data protection policies*" got the highest weighted mean with a qualitative description of Very Highly Implemented. This indicates that human resources units in the public sectors had initiated and adopted policies following the data privacy act. This further implies that many organizations were aware of the formidable threats to sensitive data in today's era. Hoel and Chen (2018) asserted that policies involving data protection are considered measures adjacent to the provisions of laws governing data security. Study also revealed the importance of crafting policy in organization that adheres to the principle of data privacy (Chua et al., 2017). Notably, item 4 "Management *of Human Resources*" got a weighted mean of 4.30 with a qualitative description of very highly implemented. This indicates that the respondents acknowledged the need to properly manage the human resources which is crucial to the realization of organizational goals. This is similar with the claim of Jacob and Farouq (2013) that in any organization, human resources served as an important asset as they determine the direction of the organization. Hence, it is important that they are properly managed.

Table 1. Level of Implementation of Data Privacy

Statements	Mean	Rank	Description
1. Organizational Security Measures	4.13	3	Highly Implemented
2. Data Protection Policies	4.38	1	Very Highly implemented
3. Records of Processing Activities	3.08	17	Moderately Implemented
4. Management of Human Resources	4.3	2	Very Highly implemented
5. Processing of Personal Data	3.25	11	Moderately Implemented
6. Contracts with Personal Information Processors	3.45	9	Highly Implemented
7. Physical Security Measures	3.72	7	Highly Implemented
8. Technical Security Measures	3.13	13	Moderately Implemented
9. Right to be Informed	3.29	10	Moderately Implemented
10. Right to Object	4.01	4	Highly Implemented
11. Right to Rectification	3.92	5	Highly Implemented
12. Right to Erasure or Blocking	3.81	6	Highly Implemented
13. Right to Damages	3.05	18	Moderately Implemented
14. Data Breach Notification	3.12	14	Moderately Implemented
15. Breach Report	3.11	15	Moderately Implemented
16. Subcontract of Personal Data	3.17	12	Moderately Implemented
17. Enforcement of DPA	3.08	17	Moderately Implemented
18. Registration of Personal Data Processing Systems	3.09	16	Moderately Implemented
19. Notification of Automated Processing Operations	3.08	17	Moderately Implemented
20. Accountability for Transfer of Personal Data	3.49	8	Highly Implemented
Over-all Mean/SD	**3.56**		Highly Implemented

Legend:

1.00 – 1.80	Not Implemented
1.81 – 2.60	Slightly Implemented
2.61 – 3.40	Moderately Implemented
3.41 – 4.20	Highly Implemented
4.21 – 5.00	Very Highly Implemented

Item 1 "*Organizational Security Measures*" (Mean=4.13), item 10 "*Right to Object*" (Mean=4.01), Item 11 "*Right to Rectification*" (Mean=3.92), item 12 "*Right to Erasure or blocking*" (Mean=3.81), item 7 "*Physical Security Measures*" (Mean=3.72) and item 6 "*Contracts with Personal Information Processors*" (Mean=3.45), got a weighted mean equivalent to highly implemented. The results imply that organizations are inclined to adopt measures and principles of data protection. Significantly, organization had initiated organizational security measures to protect sensitive information of all their employees. Bertino (2016) asserted that organizations must provide an extensive security measure which is paramount concern in the prevalent internet hacking and unauthorized disclosure of easily accessible data. This is similar with the study of Merete Hagen et al. (2008) that security measures served as an effective tool in preventing data security breaches as organization is aware of the policies, methods and procedures in the utilization of data. On the other hand, result of the item that refers to right to object indicates that human resource professionals are aware of the constitutional rights of all their employees in cases where their important data are utilized. The result further implies that they are also aware that employees have the right to control the personal and sensitive information. Control of data is obtained through the right of the subject, which in organization refers to as employees in setting up boundaries to prevent unauthorized disclosure and utilization of their data (Banubakode et al., 2022). However, Pitogo (2019) had noted that this right became a challenge to the implementation of data privacy in the Philippines because not all employees are aware of their right to control the data.

Furthermore, result refers to rectification indicates that human resource professionals are aware of the policy on data privacy relevant to the inaccuracy and error in the personal information. Pitogo and Ching (2018) noted that information and other relevant data submitted by the employees to the organization is subjected to authenticity and veracity. This may refer to the documents submitted such as that of Personal Data Sheet (PDS) and Statement of Assets and Liabilities and Net worth (SALN). However, Perez and Henninger (2022) contended that there are a lot of factors to consider in granting out this right. These includes the resources, capability, and organizational structure of the organization.

Consequently, result of the item refers to the right to erasure or blocking indicates that like the right, human resource professionals are aware of the governing privileges and compelling authority of the employees in the withdrawal and removal of personal data. However, this was argued by Connolly (2021) that right to erasure may be a compelling authority of an individual but it could be resisted to various circumstances such as the necessity of the data and overridden principle of public interest. This is also the challenged emphasized by Bernsdorff (2023) that although employees are legally subjected to this right, there are existing laws that could override so that data may be resisted to be deleted. On the other hand, result of the item that refers to physical security measures implies that organizations had instituted systems and application to secure data. Jankovic (2012) asserted that today's era of information technology, it is important for organizations to provide technical measures to map out controls related to system and security protection of available data. For most organization, physical security measures involve accessibility controls (Moses & Rowe, 2016). Additionally, result refers to contracts with personal information processors implies that organization recognized the need to hire skillful and knowledgeable personnel in the provision of data privacy. This is similar with what Bucharest Bar and Cristolovean (2022) assertion that assigned personnel must be carefully considered while ensuring compliance and regulation of the law. This is similar to Davis (2019) whose study revealed the need to provide measures following the context of the General Data Protection Regulation (GDPR).

Significantly, item 13 *"Right to Damages"* obtained the lowest weighted mean of 3.05 with a qualitative description of moderately implemented. This implies that the respondents are aware of the weaknesses and deficiencies of the organization in addressing individuals for privacy breaches. The prevalence of data breaches has been noted by Cheng et al (2017). They also revealed that organizations should seriously addressed this as this would lead to reputational damages and threats to the entirety of the organization. Notably, result supports the claim of Savelyev (2020) that there are existing gaps in the law regarding data privacy. He noted that there is inadequacy in the law pertaining to claims of damages in data protection. Previous studies also revealed the limitation of law on ensuring proper response to cases involving data breaches (Jaquemain, 2020; Knetsch, 2022).

Moreover, item 5 "*Processing of Personal Data*" (Mean=3.25), item 16 "*Subcontract of Personal Data*" (Mean= 3.17), item 8 "*Technical security measures*" (Mean=3.13), item 14 "*Data Breach Notification*" (Mean=3.12), item 15 "*Breach Report* " (Mean=3.11), item 18 "*Registration of Personal Data Processing Systems*" (Mean=3.09), item 3 " *Records of Processing Activities*" (Mean=3.08), item 17 "*Enforcement of DPA*" (Mean=3.08) and item 19 "*Notification of Automated Processing Operations*" (Mean=3.08) got a weighted mean equivalent to moderately implemented. The findings suggest that although efforts have been made to address issues and concerns relevant to data privacy, there are still notable gaps that need to be enhanced to achieve a more comprehensive approach with the law. Pitogo and

Ching (2018) asserted that the low priority agenda of organizations and agencies had posited challenges to its full implementation.

In terms of processing of personal data, this imply that organizations are aware of the complexity of processing sensitive information and data. The process involved multifaceted and critical handling pursuant to law. Saatci and Gunal (2019) asserted that certain protocols in processing personal data became a necessity in any organization. As such, Busacca and Monaca (2020) emphasized that while this is needed, the implementation became limited due to various consideration and the crucial process it takes in the organization. On the other hand, result of the item referring to subcontract of personal data, indicates that while respondents understand the provision indicated in RA 10173, they also identified that although it's allowed in the law, it should ensure that proper safeguard and confidentiality of personal data is at hand. Consent in data processing must be emphasized in the process involving subcontract of sensitive information. This is similar with argument of Puustjärvi and Puustjärvi (2016) that fragmented data such as personal health records must be properly handled following the agreement and consent of the owner.

Responses to item referring to technical security measures indicates that while they understand the need to provide sufficient measures, there are limitation in providing technical assistance in data protection. In today's changing landscape, organization must provide encryption, access control and trust management to carefully safeguard the data (Hof, 2014). However, it is argued by Mitali et al. (2022) that various limitations and vulnerabilities in security IT related mechanism hinders the implementation of this measure. Notably, Pitogo (2019) asserted that insufficiency of resources delimited the scope of agency and organization in providing appropriate and relevant measure of data protection.

Interestingly, results pertain to data breach notification and breach report indicate that organizations have established certain procedures for addressing data breaches, but there might be a need to enhance and streamline these processes. It could also imply that there is an opportunity to further clarify and strengthen the requirements and guidelines related to data breach notification and reporting within the organization. This is in consonance with Lagutina (2019) whose study revealed that organizations failed to provide effective correspondence relevant to data breaches and cases involving such. He also emphasized that to ensure strict compliance to data privacy law, organizations must provide mechanism to effective respond to issues related to data privacy and security.

As shown in Table 2, lack of awareness and emerging technologies (100 or 100%) were identified as most challenging indicators in the implementation of data privacy. This could imply that employees, at all levels, may not be sufficiently informed or educated about the importance of safeguarding sensitive information and adhering to privacy protocols. This is similar to the claim of Chua et al (2017) that lack of awareness may tend to increase the risk of non-compliance to data privacy act. As mentioned by Pitogo (2019) in his study among Local Government Units, deterrence to data privacy is the lack of awareness and understanding to the provisions of the law.

Table 2. Challenges Encountered in Data Privacy Implementation

Challenges	**Frequency n=100**	**Percentage 100%**
Lack of Awareness in DPA	100	100%
Lacks Appropriate Resources	75	75%
Complex Regulatory landscape	90	90%
Emerging Technologies	100	100%
DPO Appointment	49	49%

Significantly, emerging technologies is determined as one of the challenges that greatly affects the implementation of data privacy. The data denotes that respondents viewed the rapid advancement of technology as threat to data privacy measures. Xanthidis et al (2019) noted that emergent technologies such as Big Data, Internet of things and other social media platforms posed significant concerns to data confidentiality due to their data collection capabilities and formidable threat to data breaches. This is supported by a similar claim of Bertino (2016) whose study revealed that technologies may pervasively, effectively and efficiently collect important and sensitive data. This is the case of hacking personal data using emerging technologies (Erickson & Howard, 2007). Hence, Mohsin (2022) noted the importance of providing cybersecurity in any organization.

Moreover, almost all the respondents (90 or 90%) believed that complex regulatory landscape contributes to the non-compliance of the organization. This implies that there are laws that may override some provisions of data privacy, Hence, proper training and seminar is needed. Gonzales and Ching (2018) noted that data privacy law is multifaceted as it governs and override existing laws. This is similar with Ching and Celis (2018) whose study revealed the complexity of the law and the requirements for organizations to be compliant.

Furthermore, most of the respondents (75 or 75%) agreed that lack of appropriate resources hurdles the implementation of data privacy. This suggests that organization is baffled to effectively to implement the provision of data privacy due to resource constraint. Pitogo (2019) asserted that many organizations and agencies failed to establish a comprehensive framework of implementing data privacy because of lack of resources. This was also evident with Christen et al (2014) whose study revealed that effective implementation of data privacy needs flexible and efficient resource mechanism.

Lastly, fewer than half of the respondents (49 or 49%) considered DPO appointment as challenge to the implementation. This implies that respondents recognized the pivotal role that data privacy officer plays in the proper and effective implementation of data privacy. Data Privacy officer (DPO) is responsible in ensuring organization adheres to the data processing regulations (Kupny, 2019). Šidlauskas (2021) asserted that the appointment of DPO served as a fundamental measure of the principle of accountability enshrined in the General Data Protection Regulation (GDPR) and other relevant laws.

5. Conclusion

With the advancement of technology and innovation, several issues and concerns relevant to data privacy became prevalent. Thus, it is imperative for organization to ensure mechanism in compliance to the Data Privacy law. Furthermore, human resource management units play a very crucial role in this matter. Hence, they are considered as important part of the organization as they hold the sensitive, confidential, and personal data of the employees.

Based on the findings revealed in this study, it is hereby concluded that the implementation of Data Privacy among agencies and organizations is highly implemented. This indicates that agencies and organizations are compelled to establish a framework that complies to the provision of this law. Notably, the highest weighted mean was attributed to data protection policies, suggesting a very high level of implementation. However, despite this overall positive assessment, it is crucial to acknowledge the identified challenges. The study highlights that the right to damages emerged with the lowest weighted mean, indicating a moderate level of implementation. This underscores existing limitations within organizations in effectively addressing issues related to data breaches. Noteworthy challenges include a lack of awareness regarding the Data Privacy Act, insufficient resources, complexities in the regulatory landscape, and concerns related to emerging technologies and the appointment of Data Protection Officers (DPOs). In conclusion, while there is a commendable level of implementation in data privacy practices, addressing these challenges is imperative for ensuring comprehensive and effective data protection across agencies and organizations.

Future efforts should focus on targeted interventions to overcome these limitations and further enhance the overall data privacy framework.

6. Suggestions/Recommendations

The survey was carried out to describe the level of implementation of data privacy only. Future research may include the determination of factors that predict the implementation through regression analysis. This is to ascertain the key determinants influencing the implementation of data privacy measures within organizations. Factors such as organizational size, industry sector, leadership commitment, and regulatory compliance could be explored to understand their impact on data privacy practices. Additionally, future researcher may also compare the implementation levels of data privacy measures across different industries or organizational sizes to identify variations and identify specific challenges and strategies. Moreover, research may also improve the scope of the study since this research does not provide a greater acquisition of opinions and perceptions. Thus, this does not cover the total representative the population of Human Resource Management Officers in the Philippines.

Acknowledgement

The researcher conveys his gratitude to the Human Resource Management officers and members of the Council of Human Resource Management Practitioner of North Cotabato for completing the questionnaire and for their continued dedication to the field of Management.

References

Alafaa, P. (2022). Data privacy and data protection: The right of user's and the responsibility of companies in the digital world. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4005750

Banubakode, A., Darshi, S., & Bhalke, D. (2022). Study of data privacy and user data control. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *14*, 244–248. https://doi.org/10.18090/samriddhi.v14spli02.8

Bernsdorff, N. (2023). The protection of personal data and the "right to data deletion". *Օրինականություն / Legality*, 104–124. https://doi.org/10.59821/18294219-2023.1-nbpp

Bertino, E. (2016). Data privacy for IoT systems: Concepts, approaches, and research directions. *2016 IEEE International Conference on Big Data (Big Data)*, 3645–3647. https://doi.org/10.1109/BigData.2016.7841030

Bucharest Bar, & Cristolovean, N. M. (2022). Reflections on personal data processing that is necessary for the entering or performance of a contract. *JUS ET CIVITAS -A Journal of Social and Legal Studies*, *8*(72)(2), 37–48. https://doi.org/10.51865/JETC.2021.02.06

Busacca, A., & Monaca, M. A. (2020). Processing of personal data and AI: GDPR guarantees and limits (Between individual data and BIG DATA). In D. Marino & M. A. Monaca (Eds.), *Economic and Policy Implications of Artificial Intelligence*, (Vol. 288, pp. 51–64). Springer International Publishing. https://doi.org/10.1007/978-3-030-45340-4_6

Busch, A. (2011). The regulation of privacy. In D. Levi-Faur (Ed.), *Handbook on the Politics of Regulation*. Edward Elgar Publishing. https://doi.org/10.4337/9780857936110.00028

Chandrasekeran, I., Dharmaraj, A., Juyal, A., Shravan, M., Deb Barman, R., & Lourens, M. (2023). Cryptocurrency and data privacy in human resource management. *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 126–130. https://doi.org/10.1109/ICACITE57410.2023.10182563

Cheng, L., Liu, F., & Yao, D. (Daphne). (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. *WIREs Data Mining and Knowledge Discovery*, *7*(5), e1211. https://doi.org/10.1002/widm.1211

Ching, M. R. D., & Celis, N. J. (2018). Data privacy act of 2012 compliance performance of Philippine government agencies: A case study approach. *Proceedings of the 2nd International Conference on E-Commerce, E-Business and E-Government*, 59–63. https://doi.org/10.1145/3234781.3234784

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. https://doi.org/10.1166/asl.2018.12404

Christen, P., Vatsalan, D., & Verykios, V. S. (2014). Challenges for privacy preservation in data integration. *Journal of Data and Information Quality*, *5*(1–2), 1–3. https://doi.org/10.1145/2629604

Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics*, *34*(4), 157–170. https://doi.org/10.1016/j.tele.2017.01.008

Ciclosi, F., & Massacci, F. (2023). The data protection officer: A ubiquitous role that no one really knows. *IEEE Security & Privacy*, *21*(1), 66–77. https://doi.org/10.1109/MSEC.2022.3222115

Connolly, J. (2021). The right to erasure: Comparative perspectives on an emerging privacy right. *Alternative Law Journal*, *46*(1), 58–63. https://doi.org/10.1177/1037969X20959839

Erickson, K., & Howard, P. N. (2007). A case of mistaken identity? News accounts of hacker, consumer, and organizational responsibility for compromised digital records. *Journal of Computer-Mediated Communication*, *12*(4), 1229–1247. https://doi.org/10.1111/j.1083-6101.2007.00371.x

Foronda, S. M., Javier, N., Vigonte, F., & Abante, M. V. (2023). Implementation of Republic Act 10173 or the Data Privacy Act of 2012 in Albay Electric Cooperative (ALECO)—IMRAD. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4621933

Friedewald, M., Wright, D., Gutwirth, S., & Mordini, E. (2010). Privacy, data protection and emerging sciences and technologies: Towards a common framework. *Innovation: The European Journal of Social Science Research*, *23*(1), 61–67. https://doi.org/10.1080/13511611003791182

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. *Proceedings of the 2nd International Conference on E-Commerce, E-Business and E-Government*, 79–83. https://doi.org/10.1145/3234781.3234792

Haller, K. (2012). Data-privacy assessments for application landscapes: A Methodology. In F. Daniel, K. Barkaoui, & S. Dustdar (Eds.), *Business Process Management Workshops* (Vol. 100, pp. 398–410). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-28115-0_38

Hoel, T., & Chen, W. (2018). Privacy and data protection in learning analytics should be motivated by an educational maxim—Towards a proposal. *Research and Practice in Technology Enhanced Learning*, *13*(1), 20. https://doi.org/10.1186/s41039-018-0086-8

Hof, H.-J. (2014). Practical limitations of technical privacy protection: On the current state of IT security mechanisms used for privacy protection in the field. *Datenschutz Und Datensicherheit - DuD*, *38*(9), 601–605. https://doi.org/10.1007/s11623-014-0236-0

Jacob, J., & Farouq, S. (2013). A Review of Human Resource Accounting and Organizational Performance. *International Journal of Economics and Finance*, *5*(8), p74. https://doi.org/10.5539/ijef.v5n8p74

Jaiswal, A. (2020). The game of data and privacy. *International Journal of Advanced Academic Studies*, *2*(2), 294–296. https://doi.org/10.33545/27068919.2020.v2.i2d.395

Jankovic, D. Z. (2012). Key security measures for personal data protection in IT systems. *2012 20th Telecommunications Forum (TELFOR)*, 79–82. https://doi.org/10.1109/TELFOR.2012.6419152

Jaquemain, T. (2020). Liability of private parties for data protection breaches. In T. Kahler (Ed.), *Turning Point in Data Protection Law* (pp. 115–120). Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783748921561-115

Jha, S. (2022). Data Privacy and Security Issues in HR Analytics: Challenges and the Road Ahead. In I. Jeena Jacob, F. M. Gonzalez-Longatt, S. Kolandapalayam Shanmugam, & I. Izonin (Eds.), *Expert Clouds and Applications* (Vol. 209, pp. 199–206). Springer Singapore. https://doi.org/10.1007/978-981-16-2126-0_17

Knetsch, J. (2022). The compensation of non-pecuniary loss in GDPR infringement cases. *Journal of European Tort Law*, *13*(2), 132–153. https://doi.org/10.1515/jetl-2022-0008

Kupny, W. (2019). The role of the data protection officer in the organization's structure. *Roczniki Administracji i Prawa*, *1*(19), 295–310. https://doi.org/10.5604/01.3001.0013.3602

Lagutina, I. V. (2019). The rights of employee as a subject of personal data. *Наукові Праці Національного Університету "Одеська Юридична Академія," 18*, 110–116. https://doi.org/10.32837/npnuola.v18i0.471

Machado, P., Vilela, J., Peixoto, M., & Silva, C. (2023). A systematic study on the impact of GDPR compliance on Organizations. *Proceedings of the XIX Brazilian Symposium on Information Systems*, 435–442. https://doi.org/10.1145/3592813.3592935

Merete Hagen, J., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, *16*(4), 377–397. https://doi.org/10.1108/09685220810908796

Mitali, S., Harsh, J., Santosh, K., & Rakesh, K. (2022). Overview of data security, classification and control measure: A study. *I-Manager's Journal on Information Technology*, *11*(1), 17. https://doi.org/10.26634/jit.11.1.18557

Mohan Rao P, R., Murali Krishna, S., & Siva Kumar, A. (2021). Modern privacy threats and privacy preservation techniques in data analytics. In A. G. Hessami & P. Shaw (Eds.), *Factoring Ethics in Technology, Policy Making, Regulation and AI*. IntechOpen. https://doi.org/10.5772/intechopen.99160

Mohsin, K. (2022). Data privacy and cybersecurity. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4299439

Moses, S., & C. Rowe, D. (2016). Physical security and cybersecurity: Reducing risk by enhancing physical security posture through multi-factor authentication and other techniques. *International Journal for Information Security Research*, *6*(2). https://doi.org/10.20533/ijisr.2042.4639.2016.0077

Nerka, A. (2017). Powołanie inspektora ochrony danych jako przejaw społecznej odpowiedzialności biznesu. *Annales. Etyka w Życiu Gospodarczym*, *20*(3). https://doi.org/10.18778/1899-2226.20.3.08

Perez, P. J., & Henninger, M. (2022). The right to information: an investigation into the legal framework and implementation in the Philippines. *Proceedings of the Association for Information Science and Technology*, *59*(1), 251–261. https://doi.org/10.1002/pra2.750

Pitogo, V. (2019). Commitment on data privacy towards e-governance: The case of local government units. *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance*, 302–309. https://doi.org/10.1145/3326365.3326404

Pitogo, V. A., & Ching, M. R. D. (2018). Understanding Philippine national agency's commitment on data privacy act of 2012: A case study perspective. *Proceedings of the 2nd International Conference on E-Commerce, E-Business and E-Government*, 64–68. https://doi.org/10.1145/3234781.3234788

Pooja, P., & Greeshma, B. (2022). Human resource security in IT sector. *International Journal for Research in Applied Science and Engineering Technology*, *10*(5), 3190–3194. https://doi.org/10.22214/ijraset.2022.42978

Puustjärvi, J., & Puustjärvi, L. (2016). Managing fragmented personal data: going beyond the limits of personal health records. *Proceedings of the 9th International Joint Conference on Biomedical Engineering Systems and Technologies*, 145–150. https://doi.org/10.5220/0005626101450150

Saatci, C., & Gunal, E. S. (2019). Preserving privacy in personal data processing. *2019 1st International Informatics and Software Engineering Conference (UBMYK)*, 1–4. https://doi.org/10.1109/UBMYK48245.2019.8965432

Savelyev, A. (2020). The inadequacy of current remedies for violation of data subjects' rights and how to fix it. *Legal Issues in the Digital Age*, *2*(2), 24–62. https://doi.org/10.17323/2713-2749.2020.2.24.62

Savić, D., & Veinović, M. (2018). Challenges of general data protection regulation (GDPR). *Proceedings of the International Scientific Conference - Sinteza 2018*, 23–30. https://doi.org/10.15308/Sinteza-2018-23-30

Šidlauskas, A. (2021). The role and significance of the data protection officer in the organization. *Socialiniai Tyrimai*, *44*(1), 8–28. https://doi.org/10.15388/Soctyr.44.1.1

Warren, B. (2002). The role of the privacy officer: A portrait in the gallery of possibilities for health sciences librarians. *Journal of Hospital Librarianship*, *2*(2), 25–33. https://doi.org/10.1300/J186v02n02_03

Weber, R. H. (2015). The digital future – A challenge for privacy? *Computer Law & Security Review*, *31*(2), 234–242. https://doi.org/10.1016/j.clsr.2015.01.003

Weber, R. H., & Staiger, D. (2017). Legal and regulatory framework. In R. H. Weber & D. Staiger, *Transatlantic Data Protection in Practice* (pp. 16–61). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-55430-2_2

Wijesingha, P., & Wickremeratne, H. (2020). The role of human resources professionals on the General Data Protection Regulation. *International Journal of Scientific and Research Publications (IJSRP)*, *10*(8), 707–711. https://doi.org/10.29322/IJSRP.10.08.2020.p10489

Xanthidis, D., Alsuwaidi, F., Al Ali, M., Alolama, A., & Albaloushi, M. (2019). Information privacy and emerging technologies in the U.A.E.: Current standing and research directions. *2019 Sixth HCT Information Technology Trends (ITT)*, 314–318. https://doi.org/10.1109/ITT48889.2019.9075076