Journal of Engineering Science and Technology
Vol. 19, No. 3 (2024) 821 - 833

DEVELOPING SECURITY PRIVACY PROGRAM IN INFORMATION SYSTEM

MUHAMAD AFGHANY HARYATNO, YEFFRY HANDOKO PUTRA

Master of Information System, Universitas Komputer Indonesia, Indonesia
*Corresponding Author: afghany.75122005@mahasiswa.unikom.ac.id

Abstract

The amount of information that people generate on daily life have put their smart devices as active participants of the business that runs by numerous organizations. However, following the process the information brought numerous people to consider the safety level, as some personal information might be leaked during the process. In the last few years, there have been a lot of national and international regulations that oblige organizations to follow certain rules in their information security program. This is mainly because leakage of personal information might put the victim's privacy in danger, resulting in identity theft and perhaps financial loss. For organizations this situation could led them loss trust, reputation, and loyalty from their customers. Therefore, ensuring privacy during the process, storing, and sharing of personal information is important. Although it's clear that security and privacy are two different terms, upon implementation security often believed covers privacy too. This paper seeks to enhance information system security, by developing privacy program using privacy by design as method. The goal is to illustrate and present some insight of how privacy by design address privacy in information system security.

Keywords: Information system security, Privacy by design, Privacy program, Security.

1. Introduction

In this era, we cannot deny that Information System (IS) is easily one of a necessary thing to have, if not the most essential thing for the organizations to have [1, 2]. The amount of information that organizations generate during collecting, storing, process, and share data could be exploited to improve revenues [3]. It's fair to say that the IS has become the main source for organizations to develop their businesses. Therefore, any certain types of security breach could undermine its entire business [1]. Singaporean ecommerce cashback portal ShopBack, has been fined about S$74,400 ((US$54,600)) by Singapore's data privacy watchdog over data leak that happened in 2020 [4]. Meta, which the company that owns Facebook has been fined €265m by the Irish Data Protection Commission, after some malicious actors have accessed through a vulnerability in its tool and selling 522m user's phone numbers and email addresses in an online hacking forum [5].

Nowadays, numerous organizations commonly add personal information to their IS in order to generate certain types of data. While it may boost the business process efficiency, it poses the threats of compromising user's personal information [6, 7]. For some reasons, organizations seem to neglect the importance of protecting personal data, creating a "take it or leave it" situation for the customer or user. Meaning that the customer needs to share their personal information in exchange to use the service that organizations provide. Sadly, majority of the customer willing to give any information that organizations demand simply because they wanted to get the services, creating "privacy paradox" [8, 9]. Addressing this issue could not be done without discussing the reasons behind why organizations need to consider adding privacy into their information security program.

The purpose of information security is to make sure that organizations can continue its business by minimizing the risks and reducing the size of potential damage [2]. Therefore, it's reasonable to assert that having a secure system is necessary for an organization, which can be benefiting to improve their work [10]. Another reason is of course because the organization often processing numerous important data throughout the entire IS lifecycle, it is obvious that they need a secure system. Hence, why there are many organizations that are developing and implementing information security program. As the number of objectives to pursue continues to increase (e.g., digital marketing and recommender systems) [11], the organization nowadays seems to push further to process personal information. The customer on the other hand seems likely not to care or unaware about what is going on to their personal information. For instance, customer rarely found read moreover understand privacy policies or term and conditions provided by the organizations [12]. This situation leaves a question who is really should be the one who responsible for data privacy? Is it organization? Or the customer? [8].

Just like security, securing privacy also have to be designed, implemented, and maintained too [13]. However, there is no such a perfect system in regard addressing security, while the risks and threats are constantly evolving over the time [13]. Which is why this paper being intended to elevate the security in information security program by designing privacy program using privacy as a default. Nonetheless, developing a secure IS requires multiple complex factors to consider [14].

Over the recent period, a number of individuals and international starts to grow and more concern about privacy issues by issuing a regulation that organization

needs to follow (e.g., General Data Protection Regulation GDPR) [15, 16]. To address the privacy issues in this paper we will be using privacy by design concept by Dr Ann Cavoukian, as the concept is already popular and adopted by GDPR and ISO/IEC [17]. Privacy by design also reminds and force organization needs to be the first to address privacy issues and start to build the system around it, making privacy an essential part of an entire lifecycle [18]. In order to add privacy in information security program, understanding the definition of security and privacy is necessary; in doing so we will take a look at security and privacy in detail.

In general security can be defined as set of a practice to ensure that critical data is being protected from risk that could potentially harm the assets [19]. As already mentioned before, the advancement of IS processing large volume of data, it is necessary to provide high level of protection towards critical data that is being processed by the organization [14]. Implementing information security In IS protecting critical information is defined as information security. Apparently, while talking about addressing security there is always the three concept that is referred to, which are the confidentiality, integrity, and availability triads [4]. According to [19], there are three pillars of security which are:

i) **Confidentiality** is an information that is not disclosed to anyone unless they have been granted permission and/or authorization to do so.

ii) **Integrity** is a property or data that is accurate and not been changed or destroyed in an unauthorized or accidental manner.

iii) **Availability** is the situation of an information or data that is usable upon demand by an authorized party.

In recent years the pillars are expanded adding safety to the group to control and recognize some potential hazard that could led to certain level of risk [13]. Generally speaking, maintaining the efficiency of information security organizations must be done by addressing the potential risk and threats making the system secure from the attacks. However, the terms security in IS meant the capability to protect its information and guarantee the accuracy of the information that is being delivered [13, 14]. Mening that security can be achieved by implementing a simple old-fashioned model of security, locking up physical asset or the trust of people who worked in it [20].

Nonetheless, the important data that IS process makes them an appealing target for cyber-attacks [10]. Hence, [21] stated that security is a necessary requirement to support data privacy, to protect from unauthorized disclosure or modifications. Therefore, security stands to be an important part of securing the IS, however while the methods of processing information have been evolving, security also needs to expand its coverage and starts addressing privacy.

In broader terms privacy can be defined as state or a condition of individual that is not being observed nor disturb by others [13]. While according to [19], privacy means the ability to determine for an individual, groups, or an institution how, when and what to extent information about them to others. Furthermore [22], describe that privacy is the situation where an individual has freedom to isolate oneself and providing a segregation from others. Either way privacy in general highlights the right of an individual nor groups to stay anonymous and have a personal space upon demand. According to [23], term privacy typically pertains to disclose an individual personal information. The information that is considered as personal information are:

i) Name (e.g., full name, aliases, mother's name)

ii) Personal identifier number (e.g., credit card number, passport number)

iii) Address information (streets and/or email address)

iv) Personal characteristic (e.g., fingerprints, facial geometry, retinal scan)

v) Place of birth, race, religion, and geographic location

Having Privacy is important to people according to [8] because it carries following reasons:

i) **Psychologically**, people necessitate to have their own personal space. Having a freedom without other people judgement, allowing people to maintain their relationships with themselves.

ii) **Sociologically**, able to stay unknown and not continually being observed allowing people to be free to behave.

iii) **Economically**, people need to start protecting privacy to advance their standard of living.

iv) **Politically**, able to speak, argue and act freely, depending on their political beliefs will creates democracy amongst people.

Because security and privacy are intercorrelated with each other [23]. As a result, it is important to have a privacy program in an ISs. The question is how much protection is needed to make sure the ISs genuinely protect data privacy within its lifecycle. While it's fairly impossible to make ISs a hundred percent secure from breach and data leakage, there is no such a waste by trying to provide data privacy protection by implementing privacy by design.

Knowing that there has been a concept that was designed to look after privacy threats it feels criminal not to have it in the current ISs life cycle. Around 1990's the concept of privacy by design was developed by Dr Ann Cavoukian with the goals is to create a tool for improving data privacy provision and protection [22]. According to [17, 24] there are seven principle that is needed to consider which are:

i) **Proactive not Reactive; Preventative not Remedial**, approaching privacy risks right at the beginning of the development of ISs. Meaning that the idea is to have the system to anticipate and prevents privacy threats before it happened.

ii) **Privacy as the Default Setting**, having the ability to protect personal information without the need for action to protect it. In short, privacy is built into the system and would automatically protect the personal information and deliver the highest level of protection with no action is required because it's already built into the system.

iii) **Privacy Embedded into Design**, privacy is an essential part of ISs architecture. Ultimately, become the core of protection within the organization and adopted into the culture of the organization.

iv) **Full Functionality - Positive-Sum, not Zero-Sum**, an incremental approach to evaluate and improve the system, where all the consent is involving. Such as choosing between improving privacy or security, allowing to demonstrate that it is possible to have both rather than choosing which one.

v) **End-to-End Security - Full Lifecycle Protection**, the process of ensuring privacy extends throughout its entire life cycle. Making the process of information secure form start to finish, from collection to deletion of personal information.

vi) **Visibility and Transparency - Keep it Open**, assuring all the procession of personal data is operating under the stated promises and objectives. Providing clear and transparent to the users to trust and verify.

vii) **Respect for User Privacy - Keep it User-Centric**, beyond all of the privacy protection requirements, organization needs to consider that at the end the data belongs to the individual, while the organization might have a permission to control it, but not the ownership of the data.

The rest of this paper is organized as follows. Section I provides a quick background of why organizations need to start addressing privacy and enhancing their security systems. Section II discusses the methodology that is used to guide this paper to design privacy program in IS lifecycle. Section III will start by showing the relevance of security and privacy, followed by designing privacy program that applied using Plan Do Check Act (PDCA) cycle. Furthermore, the section will discuss about the assessment of threats and risks related to implementation of privacy program.

2. Research Method

This study employs qualitative research methods to investigate the interpretations and the essential of security and privacy in IS lifecycle. Literature study conducted in this paper intend to collect data and information related to the topic, which later serve as a support of this study by attains greater understanding about the topic. The majority of the data source obtained through online journal, paper and book that have credibility. Before being used as a basic knowledge of this study the data will be analysed and read by the author.

3. Results and Discussion

3.1. Towards implementing security and privacy

Before implementing security and privacy in IS life cycle, recognizing the boundaries and overlap between security and privacy can be very crucial, as it would giving us the insight and finding the gaps that need to be achieved [23]. According to [13, 19], security and privacy share its relationship on their risk.

From Fig. 1 we can clearly see that any threats to confidentiality, integrity and availability which include personal information are considered as security and privacy risks. Implementing privacy by design for organizations can be done by designing a specifications and recommendations that can be used for the company for a variety of projects [17].

As already mentioned earlier there are three critical pillars of security, which are confidentiality, integrity, and availability. Table 1 depicts the difference in objectives according to [23] regarding security and privacy.

After understanding the objectives differences between security and privacy, before we begin developing the system, we need to look at implementation of security by design and privacy by design by [24], how privacy by design principles is covering security and privacy.

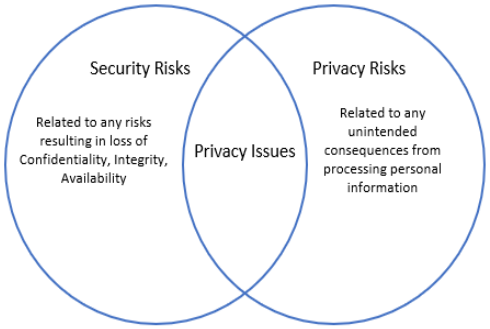

Fig. 1. Security and privacy.

Table 1. Confidentiality, integrity, and availability.

	Security	**Privacy**
Confidentiality	Focuses more on processes and appliance with the intention to prevent unauthorized access	Make sure that personal information only disclosed according to the purpose of collection
Integrity	Protecting the data from changing itself by authorized or unauthorized individuals to make sure the accuracy of the data	Aims to guarantee that there is no change of personal information without permission of the user
Availability	Puts effort into ensuring that authorized user able to have timely access to the data when it's needed	Focus on achieving the ability of the user to access their personal information and exercise their rights (e.g., data access and deletion)

Table 2. Security by design and privacy by design.

Privacy by Design Principles	**Security** **Protect people and organization assets**	**Privacy** **Protect and respect personal information**
Proactive not Reactive; Preventative not Remedial	Starts with the security concept, and utilize it to guide the proactive implementation of security	Avoid waiting privacy vulnerabilities to become real threat to the organization by anticipate and preventing it from the beginning of the development
Default Setting	Implement the basics of security by design, including segregation of duties and access control to ensure the confidentiality, integrity, and availability of the assets	Develop the privacy built into the system by default to protect personal information automatically.
Embedded into Design	Leverage software security assurance	Acknowledge privacy as an essential part of the system and develop the system around it,

Privacy by Design Principles	Security Protect people and organization assets	Privacy Protect and respect personal information
	practice to ensure the security of the asset	until eventually privacy becomes culture of the organization
Full Functionality-Positive Sum, not Zero Sum	Seek the win-win solution for any risks regarding the security threats.	Make provisions to all consent in a positive-sum and applying it incrementally to make sure all the consent is addressed
End-to-End Security-Full Lifecycle Protection	Guarantee the confidentiality, integrity, and availability of all the assets for all stakeholders	Make sure the privacy protection from the beginning of the process until the end
Visibility and Transparency-Keep it Open	Advancing the security by implementing widely acknowledge standard and establish protocols to ensure the security	Keep all the process visible to the user, providing clear and transparent of the process
Respect for User Privacy-Keep its User Centric	Security must cover organization and individual interest and protecting it from security risks.	Respect user interests and protect any individual information , keep it user centric.

From Table 2 it can stated that, the main difference of developing security program and privacy program is about protecting the type of data. Which security program mainly focused on organization information assets, and privacy program mostly attentive to protection of personal information. Figure 2, according to [23] will represents the key areas that becomes concern of privacy program.

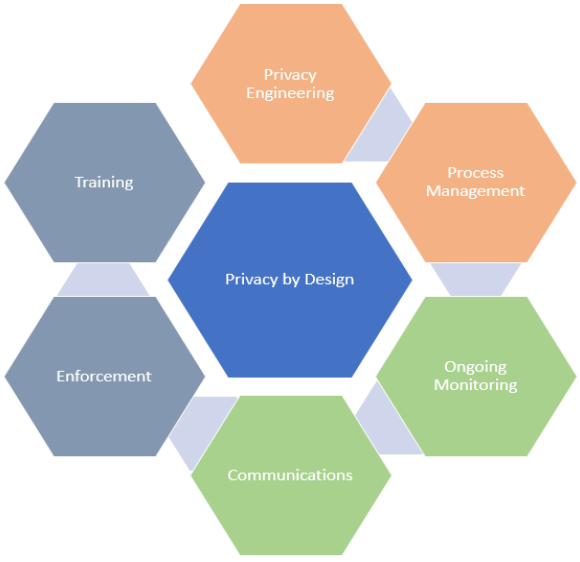

Fig. 2. Privacy by design.

i) **Privacy by Design** is the central component of key areas of privacy programs. It enforces the organization to have privacy designed into the system before the implementation begins.

ii) **Privacy Engineering** encompasses the implementation and implementation of ongoing privacy operation and management. The main goals of privacy engineering are:

   a) Combine functionality and management practices to fulfil privacy requirements.

   b) Preventing the compromise of personal information

   c) Mitigate the impact of personal data breach

iii) **Process Management**, ensuring privacy is coordinated within the organization on all sectors.

iv) **Ongoing Monitoring**, monitoring the performance of the protection of personal information privacy and measure the result of privacy controls that applied.

v) **Communications**, all of the knowledge about privacy awareness, policy and procedures have to be communicated within the organization and external stakeholder and interested parties.

vi) **Enforcement**, detecting privacy breach and enforcing the organization to follow privacy procedures

vii) **Training**, train all employees to protecting privacy related documents and data

From Fig. 2 it can be stated that privacy by design plays a major role in designing privacy program, therefore in Fig. 3 will depicts PDCA cycle as a basic concept to implement privacy by design for privacy program.

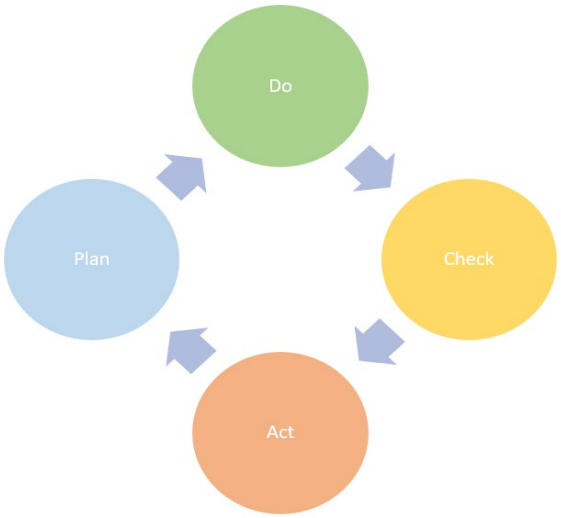

Fig. 3. Plan, do, check, act.

i) **Plan:** In the first phase of the development of privacy program, the organization will have to determine the objective, scope policies, and priorities of the privacy program. In this phase the organization can utilizing the seven principles of

privacy by design as a guidance. Which can assist organizations to design the system that able to handle risks before it occurs. Moreover, the seven principles of privacy by design will force the organizations to consider maintaining protection from end-to-end.

ii) **Do:** Second phase of the development of privacy program, the organizations need to start implementing all the plans that have been made. Also, starts to train awareness and education about privacy protection to all the employees. During the implementation, organizations need to record and save all of the operations for further examination and evaluation.

iii) **Check:** The third phase of the development of privacy program, the organizations need to conduct internal audit and management evaluation. This phase is very essential because the efficiency and effectiveness of the operation will be measured and starts addressing what went wrong during the process of implementation.

iv) **Act:** The fourth phase of the development of privacy program is implementation, the organizations will continue the program according to the result of previous phase. Each department have to conduct maintenance and improvement to all the process. Mainly to ensure the continuity of the program by assessing and verifying the efficacy of corrective and preventive measures. While doing so, the organization also need to make sure that all the processes are operating under the stated promises and objectives of privacy protection.

After designing privacy program using PDCA, the implementation of the privacy program will have threats and risks that might occur in the future. Therefore, to prepare mitigation for the risks and threats, needs to conduct privacy risk assessment. With the intention to evaluate and improve its privacy program, as the threats and risks always evolving.

3.2. Privacy risk assessment

The main objective of the implementation of privacy program is to enable the organization to maintain and determine the appropriate solutions to protect information privacy. To have a better understand of the privacy risk, Table 3 according to [23], will represent four essential elements that need to consider when addressing privacy risk.

According to [23], the solution to address the issues caused from these four elements can be done by these three steps:

i) Determine the possible threats and risks related to privacy assets and starts correlation it the user to measure the impact that could potentially happened if the threats and/or risks occurs.

ii) Identify privacy incidents that happen to actually violates the privacy of personal information.

iii) Measure likelihood of the privacy incidents that happened in the past and starts grouping the incidents by its impact.

After understanding some of the essential risks and threats when addressing privacy protection, we represent the implementation of privacy by design that can be implemented in the organization information lifecycle.

Table 3. Privacy risk.

	Risk	Example
Privacy-related asset	Generally personal information of employees, customer, clients, etc.	Patient's medical record stollen by unauthorized individual or group.
Privacy threats	A possibility of a privacy breach that arises during the situation of procession of personal information that can cause harm to an individual	Leakage of personal information that includes sensitive information (e.g., retina scan, fingerprint)
Privacy vulnerability	Some weaknesses in the system that could potentially exploited by unauthorized user, which can compromise user's privacy.	A staff or member of the organization who should not be able to access other's personal information, but due to inadequate access control they are able to do so.
Privacy controls	Operational, procedures and technical controls, that intended to protect personal information and ensuring compliance with organization regulations	User's personal information leaked due to robust system and the stored data is not encrypted.

3.3. Implementation of privacy by design strategies

In this section we will be discussing about the strategies that generated using privacy by design method according to [25], that can be implemented within the organization information lifecycle.

3.3.1. Data-oriented strategies

i) Data Minimization can be utilized to limiting the collection of personal information, and only collecting essential data that can support personal data procession. Therefore, it can limit the chance of breach moreover misuse of personal data.

ii) Hide, upon storing collected personal information it highly recommends to masking them from bare view and hide it from other parties that doesn't have any authority. Some of the best practices to do so is the pseudonymization replacing identifying information with aliases, with the goal to make data less identifiable.

iii) Separate, when it comes to collecting personal information there are many types of personal information that can be collected. In that way separating personal information by type can be beneficial as several data might contains sensitive personal data that needs to get encrypted before storing it in database. By doing so it can prevent leakage of personal information as breach that didn't leak personal information is not count as data leak.

3.3.2. Process-oriented strategies

i) Communication, upon processing personal information transparency and ensures an up to date to the owner of personal information is must. In intentions to comply with regulations and standards.

ii) User access limitation, not all of organization employees needs to understand nor have access to user's personal information, only authorized user and employees that granted permission that can do it.

iii) Control, collecting personal data might help organizations to achieve their goals, but we have to keep in mind that 'keep it user centric' because organizations definitely not the owner of the personal information but user are. Therefore, granting them to manage their personal information and selecting what information they willing to share to the organization.

However, these are just a few risks and solutions while in the real case scenario there are numerous privacy risks that might occur during the implementation. Privacy is an important part of foundations humans' life as already discussed by [8]. While on the organization perspective protecting privacy can provide benefits for them such as building customer trust and protecting their assets. However, implementing security and privacy might be a challenging activity to do as the constant change within the industry itself and the definition of security and privacy.

This paper shows that privacy by design can actually become an effective and efficient foundation to address security and privacy within the organizations [17]. Although, some of the privacy by design goal is to have the system automatically handle the security and privacy issues without having to do anything in particular, constantly reviewing the risk and solution will keep the system stays relevant.

Despite all that, in real case scenario there is a situation where organization might already have a decent infrastructure of IS lifecycle, but the employees does not know how to implement it. Therefore, looking at the article by [16], a proper well explained how to implement must be defined and delivered to the people in charge. Which means that not only organizations need to develop a security privacy-based system but there is also having to be an instruction of how to implement it. On top of all that the employees also need to get trained to ensure they are aware of security and privacy issues.

4. Conclusion

In the end of the day, organizations and user need to start recognizing the importance of protecting personal information. This paper has illustrated how can the organization elevate their security by addressing privacy concerns using privacy program, that is implemented from the beginning of their IS lifecycle. It is important to consider that there is no such a perfect system that could handle privacy issues without having to improve and evaluate its system. Having privacy by design built along with the IS lifecycle is recommended, yet if the employees do not know how to implement and operate it becomes impracticable. In spite of that it is important to examine the employee's capacity and competencies in order to make the system useful. The fact that privacy by design is able to handle the privacy issues, or at least mitigating and preventing privacy leakage, however there is nothing wrong to elevate the privacy concern beyond privacy by design.

Future work is recommended to combining privacy by design and privacy engineering. As privacy by design is intended to design the privacy program, and the implementation is managing by privacy engineering. Also future research can start addressing regulations like GDPR or standards that manage privacy protection like ISO 27701. The advancement the framework would be combining Information Security Management System ISMS and Privacy Information Management System PIMS, together with the aim of implementing both security and privacy and making it as a culture in the organization. Privacy by design itself has already been adopted by ISO/IEC 27701, so advancing further research to PIMS seems already streamlined.

References

1. Zaydi, M.; and Nasserddine, B. (2016, October). Information system security governance: Technology intelligence perspective. *Proceedings of the* 2016 *International Conference on Advanced Communication Systems and Information Security* (*ACOSIS*) 1-6.
2. Aleksandrova, S.V.; Vasiliev, V.A.; and Aleksandrov, M.N. (2020, September). Problems of implementing information security management systems. *Proceedings of the* 2020 *International Conference Quality Management*, *Transport and Information Security*, *Information Technologies* (*IT&QM&IS*) 78-81.
3. Martinelli, F.; Saracino, A.; and Sheikhalishahi, M. (2016, August). Modeling privacy aware information sharing systems: A formal and general approach. *Proceedings of the* 2016 *IEEE Trustcom*/*BigDataSE*/*ISPA* 767-774.
4. Cheryl, B. K.; Ng, B. K.; & Wong, C. Y. (2021). Governing the progress of internet-of-things: ambivalence in the quest of technology exploitation and user rights protection. *Technology in Society*, 64(1), 101463.
5. Rubinstein, I.S.; and Good, N. (2013). Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents. *Berkeley Technology Low Journal*, 28(1), 1333-1341.
6. Patra, L.; and Rao, U.P. (2016). Internet of Things - Architecture, applications, security and other major challenges. *Proceedings of the* 2016 3*rd international conference on computing for sustainable global development* (*INDIACom*). 1201-1206.
7. Tripathi, M.; and Mukhopadhyay, A. (2020). Financial loss due to a data privacy breach: An empirical analysis. *Journal of Organizational Computing and Electronic Commerce*, 30(4), 381-400.
8. Abdullah, H. (2021). Towards the development of an information privacy protection awareness initiative for data subjects and organizations. *Proceedings of the* 2021 *National Computing Colleges Conference* (*NCCC*) 1-7.
9. Balapour, A.; Nikkhah, H.R.; and Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, 52, 102063-102070.
10. Muhasin, H.J.; Gheni, A.Y.; and Yousif, H.A. (2022). Proposed model for data protection in information systems of government institutions. *Bulletin of Electrical Engineering and Informatics*, 11(3), 1715-1722.

11. Saatci, C.; and Gunal, E.S. (2019). Preserving privacy in personal data processing. *Proceedings of the* 2019 1*st International Informatics and Software Engineering Conference* (*UBMYK*) 1-4.
12. Pleger, L.E.; Guirguis, K.; and Mertes, A. (2021). Making public concerns tangible: An empirical study of German and UK citizens' perception of data protection and data security. *Computers in Human Behavior*, 122(1), 106830-106838.
13. Manditereza, P.T.; and Bansal, R. (2016). Renewable distributed generation: The hidden challenges–A review from the protection perspective. *Renewable and Sustainable Energy Reviews*, 58(1), 1457-1465.
14. Akatov, M.S.; Safonov, S.N.; and Tuv, A.L. (2020). The organization of information protection at the object of informatization. *Proceedings of the* 2020 *International Conference Quality Management*, *Transport and Information Security*, *Information Technologies* (*IT&QM&IS*), 137-139.
15. Swartz, P.; Da-Veiga, A.; and Martins, N. (2019). A conceptual privacy governance framework. *Proceedings of the* 2019 *Conference on Information Communications Technology and Society* (*ICTAS*), 1-6.
16. Polkowski, Z. (2018). The method of implementing the general data protection regulation in business and administration. *Proceedings of the* 2018 10*th International Conference on Electronics*, *Computers and Artificial Intelligence* (*ECAI*), 1-6.
17. Cavoukian, A. (2020). Understanding how to implement privacy by design, one step at a time. *IEEE Consumer Electronics Magazine*, 9(2), 78-82.
18. Foukia, N.; Billard, D.; and Solana, E. (2016, December). PISCES: A framework for privacy by design in IoT. *Proceedings of the* 2016 14*th Annual Conference on Privacy*, *Security and Trust* (*PST*), 706-713.
19. Leszczyna, R. (2018). Cybersecurity and privacy in standards for smart grids–A comprehensive survey. *Computer Standards and Interfaces*, 56(1), 62-73.
20. Liu, X.; Ahmad, S.F.; Anser, M.K.; Ke, J.; Irshad, M.; Ul-Haq, J.; and Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*, 13(1), 927398-927404.
21. Hathaliya, J.J.; and Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications*, 153(1), 311-335.
22. Markopoulou, D.; Papakonstantinou, V.; and De Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law and Security Review*, 35(6), 105336-105342.
23. Aljeraisy, A.; Barati, M.; Rana, O.; and Perera, C. (2021). Privacy laws and privacy by design schemes for the internet of things: A developer's perspective. *ACM Computing Surveys* (*CSUR*), 54(5), 1-38.
24. Arfaoui, S.; Belmekki, A.; and Mezrioui, A. (2021). A privacy by design methodology application in telecom domain. *International Journal of Communication Networks and Information Security*, 13(2), 184-198.
25. Semantha, F.H.; Azam, S.; Shanmugam, B.; Yeo, K.C.; and Beeravolu, A.R. (2021). A conceptual framework to ensure privacy in patient record management system. *IEEE Access*, 9(1), 165667-165689.