Singapore Polytechnic

ASSIGNMENT COVER SHEET (GROUP No.5)

Please complete and attach this form to your assignment cover page.

All assignments must be submitted to lecturer on the stipulated submission date.

Name 1:	Kho Li Hao	Admission No. 1:	P2341756
Name 2:	Aung Kaung Chit	Admission No. 2:	P2339728
Name 3:	Russell Chin	Admission No. 3:	P2322357
Name 4:	Hoi Damien	Admission No. 4:	P2304090

Module Name:	Data Protection for Cyber Security
Module Code:	ST2420
Class:	DISM/FT/2B/02
Lecturer's Name:	Mr. Yeo Jun Hao
Topic/Titles:	PDPA vs GDPR - Understanding the nature of the personal data
Assignment No. (i.e., 1, 2,3):	1

Your assignment should meet the following requirements.

Please confirm this by ticking ☑ the boxes before submitting your assignment.

- ☑ Proper report structure including cover page, content page and documentation of your work, Reflection (1 page per group member) and task allocation.
- ☑ Font: **Arial**; Font Size: **12**; Alignment: **Justify**
- ☑ The first page of my/our assignment is clearly labelled with (group no.), my/our name/s, student number/s, class, module name, module code, Lecturer's name, Topic/Titles and (Assignment No.).
- ☑ I/We have retained a copy of my/our assignment
- ☑ I/We have completed and signed the declaration below

Declaration of Academic Integrity

Academic Integrity is a central tenet of Singapore Polytechnic. The polytechnic rules state that "Cheating in examinations and other assessed work is a very serious offence. This includes copying and using plagiarised material. Any student who cheats, attempts to cheat or breaches any rules for examinations and tests will face disciplinary action. The student is liable to be expelled." Check options below:

☑ I affirm that the work I submit is my own, produced without help from any AI tool(s).

which I have acknowledged fully. By signing this form, I declare that the above affirmation made is true, and that I have read and understood the rules stated in Students Handbook on "Plagiarism" and "Breach of Examination/Assessment Rules".

Name: Aung Kaung Chit **Student ID**: P2339728

Signature:  **Date**: 24/11/2024

All forms of plagiarism, cheating and unauthorised collusion are regarded seriously by Singapore Polytechnic and could result in penalties including failure in the module and possible exclusion from the Singapore Polytechnic. If you are in doubt, please contact your Lecturer

Table of Contents

Introduction

In today's digital landscape, the protection of personal data has become a critical concern for both individuals and organizations alike. With the ever-increasing reliance on data-driven technologies and cross-border transactions, understanding how personal data is defined and regulated under different legislations is vital for ensuring compliance and safeguarding privacy.

Our team chose the topic "PDPA vs GDPR: Understanding the Nature of Personal Data" because it emphasises the foundational principles of two data protection legislations that govern the collection, use, disclosure and care of personal data: Singapore's Personal Data Protection Act (PDPA) and European Union's General Data Protection Regulation (GDPR). This topic resonates with our coursework in Data Protection for Cyber Security and allows us to compare the rules and concepts that govern personal data globally.

By analysing similarities and differences, we hope that our research provides insights that enhance understanding and foster awareness of the challenges organisations face when dealing with personal data across different jurisdictions. Additionally, this topic holds practical value for businesses operating internationally as understanding these regulations is a must for maintaining compliance and protecting stakeholder trust.

Definition

Personal Data

The PDPA defines personal data as data about an individual who can be identified from that data or other accessible information. It does not distinguish special categories of personal data, treating all types uniformly. However, sensitive data like medical or financial information may require additional safeguards. This includes names, NRIC numbers, and contact details. The focus is on protecting identifiable information within Singapore.

The GDPR however, takes a broader approach by defining personal data as any information that directly or indirectly identifies a natural person. This includes names, identification numbers, online identifiers, and location data. Additionally, the GDPR specifies special categories like racial origin, health data, and biometric information, which are subject to stricter processing requirements.

Pseudonymisation

The GDPR defines pseudonymised data as personal data that can no longer be assigned to a specific individual without the usage of supplementary information, provided that such information is isolated and confirmed that the personal data cannot be assigned to an identifiable individual.

The PDPA, on the other hand, does not have a definition for pseudonymised data. Instead, it describes pseudonymisation as replacing identifiable data with fabricated values that can or cannot be reversed.

Scope

Personal Scope

Both the PDPA and GDPR are meant to protect individuals' personal data, and there are some underlying similarities between them. The GDPR only protects living individual’s personal data and deceased individual’s personal data are not protected. For PDPA, it also only protects living individual’s personal data and generally does apply to deceased individuals with the exception of some limited circumstances, whereby the individual has been dead for 10 years or fewer, or personal data that is contained in a record has surpassed 100 years in existence, regardless of whether the data subject is alive or dead.

The most prominent difference for personal scope between GDPR and PDPA is that GDPR applies to both the private sector, such as businesses, and the public sector, such as government agencies. Whereas for PDPA, public agencies are excluded, as well as any organisations that act on behalf of public agencies. Additionally, the GDPR protects all living individuals as long as they are in EU, regardless of nationality or place of residence. As compared to the PDPA, which focuses on the governing of use, collection and disclosure of personal data of individuals of Singapore, regardless of their nationality or residence.

Territorial Scope

The territorial scope refers to where the law would be applicable, specifically the geographical boundaries where organisations must comply. Both the GDPR and PDPA are similar in terms of their territorial scopes.

For GDPR, it applies to all entities or organisations that are present in the EU. Even if data processing occurs outside the EU's boundaries, the GDPR still needs to be complied as long as the data processing is correlated to the activities of the establishment in the EU.

For PDPA, it applies to all organisations, except public agencies, in Singapore that are collecting, using or disclosing personal data in Singapore. Additionally, the GDPR extends its scope to include organizations outside the EU if they offer goods or services to EU residents or monitor the behavior of individuals within the EU.

Similarly for PDPA, The PDPA focuses on activities involving personal data in Singapore, regardless of whether the organization handling the data is local or foreign, registered in Singapore, or has a physical presence in the country.

Material Scope

The material scope of a data protection regulation defines the types of activities and data it governs. Both the PDPA and GDPR are similar when it comes to processing data for domestic and personal use only, as they are both excluded from application. The GDPR also excludes its application if data processing is done for law enforcement or national security, and similarly for PDPA, it is also excluded for public agencies, or organisations acting on behalf of public agencies, which include the Government and its ministries or departments. Other aspects of material scope, however, are different between the PDPA and the GDPR. The PDPA does not make a distinction between different types of personal data, whereas the GDPR identifies special categories of personal data. Furthermore, the PDPA does not distinguish between automated and non-automated methods of data processing, in contrast to the GDPR.

Accountability and Obligations

Both GDPR and PDPA highlight the importance of accountability in data protection by requiring organisations to construct frameworks and procedures that preserve the rights and privacy of individuals

Accountability Under GDPR

The GDPR includes accountability as a key principle, which mandates that organizations not only comply with its data protection rules but also be able to demonstrate their compliance. This involves maintaining adequate documentation, developing data protection policies, and ensuring lawful data processing.

Organizations engaging in activities such as large-scale data processing, monitoring of individuals, or handling sensitive information must appoint a DPO. The DPO serves as an advisor on compliance matters, ensures adherence to GDPR rules, and acts as a liaison with supervisory authorities. High-risk activities like profiling or processing sensitive data require Data Protection Impact Assessments (DPIAs). These assessments evaluate potential risks to individual rights and outline measures to mitigate them.

The GDPR requires organizations to adopt measures such as data encryption, pseudonymisation, and secure access controls to protect personal data and ensure its integrity and confidentiality. Organizations, particularly those conducting high-risk or large-scale processing, must keep detailed records of their activities, including data retention periods and purposes of processing. Exceptions apply to smaller organizations under specific circumstances.

The GDPR requires organizations to report data breaches to the appropriate authorities within 72 hours, provided the breach could impact individuals' rights. Affected individuals must also be informed if the risk is significant.

Accountability Under PDPA

The PDPA outlines an accountability obligation for organizations, requiring them to implement practices and policies to manage personal data responsibly and in compliance with its provisions.

All organizations must designate at least one DPO to oversee data protection matters. This individual's contact details must be made publicly available to handle queries and complaints. The PDPA allows for the appointment of multiple DPOs or a team to fulfill these responsibilities. Organizations are required to establish and enforce policies for handling personal data. These policies should include procedures for managing requests to access or correct data.
Data Protection Impact Assessments (DPIAs). DPIAs are necessary in specific cases, such as when organizations process data based on deemed consent or legitimate interests. These assessments identify and address potential risks to individuals' privacy.

The PDPA mandates organizations to implement security measures to prevent unauthorized access, modification, or misuse of personal data. Encryption, secure networks, and access controls are among the recommended safeguards. Organizations must ensure data accuracy and retain it only for as long as necessary to fulfill its original purpose or comply with legal obligations.

The PDPA requires organizations to notify the Personal Data Protection Commission (PDPC) of significant breaches, particularly those that could cause harm or affect a large number of individuals.

Challenges in Data Protection

In today's hyperconnected world, the complex interactions between technology, regulatory frameworks, and organizational agendas give rise to data protection concerns. Data protection becomes a difficult issue requiring technical complexity, legal compliances, and ethical obligation as its volume and diversity increase exponentially. Proactive and flexible security measures are necessary due to evolving dangers including insider threats and cyberattacks. Organizations must simultaneously manage divergent international laws and user demands for openness and privacy. Businesses must carefully balance innovation, operational effectiveness, and protecting sensitive data in this constantly shifting market.

Compliance with Multiple Jurisdictions

When it comes to maintaining compliances for companies, Personal Data Protection Act (PDPA) of Singapore and General Data Protection Regulation (GDPR) are met with a series of challenges. Both frameworks plan and aim to better safeguard and protect personal data in their scope, businesses are finding it challenging to comply with it due to circumstances and particular criteria.

The General Data Protection Regulation (GDPR) gives people complete control over their personal data, including the power to object to processing, erase their data, and transfer their data. People have considerable control over their personal information thanks to these rights. However, unlike the GDPR, the PDPA does not give the same breadth of individual rights and instead focuses more on permission and data retention. While companies must designate a Data Protection Officer (DPO) under both frameworks, the GDPR places stricter demands on the DPO's independence and level of experience, while the PDPA gives companies greater flexibility, including the choice to designate a DPO who works in a team.

The cost of compliance is also a significant concern. Extensive obligations of the GDPR such as appointing Data Protection Officers (DPOs), conducting Data Protection Impact Assessments (DPIAs), and maintained detailed processing records which often requires greater resources compared to PDPA compliance.

Handling Cross-Border Data Transfers

For businesses that operate across borders, cross-border data transfers provide a significant issue, especially when it comes to managing compliance with regulations such as the General Data Protection Regulation (GDPR) of the European Union and Singapore's Personal Data Protection Act (PDPA). Although protecting personal data during international transfers is the goal of both frameworks, their standards and methods are very different.

The GDPR sets strict rules on cross-border transfers, making it illegal to send personal information to nations outside the European Economic Area (EEA) unless the recipient nation guarantees a sufficient degree of data protection. However methods such as the Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or authorized codes of conduct and certifications allows it. Additionally, transfers may be permitted by law if data subjects give permission explicitly. The purpose of these measures is to provide data protection standards that are on par with those in the EU.

As long as the organization ensures that the receiver offers a level of protection adequate to the PDPA, cross-border transfers are permitted under the law. This can be accomplished by relying on recipient nation legislation that comply with PDPA requirements, obtaining legally binding agreements, or obtaining certifications such as the APEC Cross-Border Privacy Rules (CBPR). The PDPA provides greater flexibility than the GDPR, enabling businesses to customize protections to meet their business requirements.

Cybersecurity Implications for Personal Data Protection

Cybersecurity plays an essential role in protecting and safeguarding personal data under the regulations like the Personal Data Protection Act (PDPA) and the General Data Protection Regulation (GDPR). Effective cybersecurity measures are crucial to preventing breaches that might compromise sensitive personal data as businesses are relying more on digital systems for data collecting, processing, and storage.

Organizations are required by the PDPA and GDPR to safeguard personal data against theft, misuse, and unauthorized access. Data breaches are frequently caused by cybersecurity flaws such as insufficient encryption, unpatched systems, and weak access controls. Organizations are required under the GDPR to notify supervisory authorities of breaches that endanger the rights and freedom of individuals within 72 hours. Additionally, organisations are required to learn and adopt technical skills such as encryption, firewalls and intrusion detective systems to safeguard personal data.

While cybersecurity technologies are vital and important, subsequent errors such as human errors can also lead to a data breach. Both frameworks emphasizes the importance of training their employees and ensure that they are aware on how to mitigate. Failing to do so would lead to employees falling victim to phishing attacks or having misconfiguration problems in the system which ultimately lead to exposing of personal data.

Key Differences

Consent Requirements

Consent is a foundational principle in both PDPA and GDPR, but their approaches to obtaining and using consent differ significantly.

Under the PDPA, organizations must obtain the individual's explicit consent before collecting, using, or disclosing their personal data. Consent is key to data processing, with specific exceptions such as deemed consent by notification or legitimate interests introduced in the 2021 amendments. For example, deemed consent applies when an individual voluntarily provides data for a specific purpose, and legitimate interest applies when the benefits outweigh risks to the individual, subject to appropriate safeguards.

In contrast, the GDPR offers several legal bases for data processing beyond consent. These include contractual necessity, compliance with legal obligations, protection of vital interests, performance of tasks in the public interest, and legitimate interests pursued by the data controller. While consent remains an essential basis, it is not the sole requirement, providing organizations with flexibility in justifying data processing.

Data Subject Rights

The GDPR and PDPA differ significantly in the extent of rights granted to individuals regarding their personal data. The GDPR provides a comprehensive framework of rights that empower individuals to control how their personal data is used, while the PDPA focuses on more basic protections. The GDPR grants individuals extensive rights concerning their personal data, reflecting its focus on empowering individuals and promoting transparency. The PDPA, while offering similar protections, does not provide the same breadth of rights. Rights such as data portability, objection to processing, and the right to erasure are not explicitly included under PDPA.

Data subjects are given a number of important rights under the GDPR. The Right to Access guarantees transparency in data processing by enabling people to see and comprehend how their data is being processed. People can request that any erroneous or incomplete data stored by an organization be corrected under the Right to Rectification. Furthermore, the Right to Erasure, sometimes known as the "Right to Be Forgotten," allows people to ask for the erasure of their personal information in certain situations, such as when it is no longer required for the reasons it was gathered. The GDPR also establishes the Right to Data Portability, which enables people to move their personal information across companies in a machine-readable, organized, and widely-used manner. Last but not least, the Right to Object allows people to object to certain data processing practices, like profiling or processing for direct marketing.

The PDPA, on the other hand, guarantees a more constrained list of rights. It includes the Right to Access, which enables anyone to ask for access to the personal information that an organization has about them. In a similar vein, people can ask for changes to any inaccurate information in their records under the Right to Correction. However, rights like data portability, objection to processing, and erasure of personal data are not specifically covered by the PDPA.

While both frameworks aim to protect data subjects, the GDPR offers a broader and more detailed set of rights, empowering individuals with significant control over their personal data. The PDPA, in comparison, provides fundamental rights but does not match the depth or range of protections offered under the GDPR.

Enforcement and Penalties

Both GDPR and PDPA enforce strict compliance through penalties, though the scale and scope of these penalties differ.

The PDPA allows the Personal Data Protection Commission (PDPC) to impose fines of up to SGD 1 million for serious breaches. Organizations with annual turnovers exceeding SGD 10 million may face fines up to 10% of their turnover for significant breaches, reflecting increased emphasis on accountability in recent amendments.

The GDPR imposes much higher penalties, with fines reaching up to €20 million or 4% of the global annual turnover, whichever is higher. The two-tier fine system allows regulatory authorities to impose lower fines for less severe breaches and maximum fines for violations of core principles such as consent, data subject rights, or cross-border data transfers.

As you can see, the GDPR’s penalty structure is far more severe, reflecting its global application and the EU’s strong emphasis on data protection as a fundamental right.

PDPA vs GDPR : Relation to Data Protection for Cyber Security

It is crucial to have effective data protection in safeguarding individual's privacy rights and building trust in digital services. Consequently, data protection laws like GDPR and PDPA play pivotal roles to shape how organisations design and implement their cybersecurity strategies to minimize legal risks.

PDPA and GDPR's Impact on Cybersecurity Strategies

Although PDPA and GDPR bear several similarities and differences with regard to scopes, terminologies and enforcement mechanisms, both frameworks share common interests of protecting personal data and significantly influence the development of cybersecurity strategies by emphasizing robust protection and compliance mechanisms.

Both GDPR and PDPA encourage the organizations to integrate data protection principles into system design, called privacy by design, and both frameworks underline the need for data security measures such as encryption, pseudonymization, secure access control mechanisms and regular audits for maintaining the confidentiality, integrity and availability of personal data.

Moreover, focusing on risk management such as conducting Data Protection Impact Assessment (DPIA) in compliance with GDPR and PDPA also enhances cybersecurity readiness. For example, a financial service company ABC identifies that a DPIA is needed to implement while deploying a customer relationship management platform that collects and processes large volumes of personal and financial data. The assessment may outline several potential risks, such as unauthorized access to sensitive data or no consent withdrawal or even exposure to data breaches. Hence, the need to enforce security measures and incident response plans to mitigate these risks strengthening cybersecurity readiness.

Ensuring Compliance in Cybersecurity Frameworks

Since ensuring compliance with GDPR and PDPA frameworks is pivotal for organisations to maintain trust and avoid legal repercussions, embedding compliance into cybersecurity frameworks is considered to be the first priority for the organisations. Consequently, organisations can systematically address vulnerabilities and enhance their data protection capabilities.

Organisations are encouraged to conduct regular audits and these evaluations can verify the implementation of appropriate security measures and detect deviations from the compliance standards. As a result, organisations can assess technical and organisational security measures to ensure data security and monitor personal data handling practices.

What’s more, the accountability principle of PDPA and GDPR ensures that organisations implement data governance policies establishing clear protocols for data ownership, storage and access control. Complying with the provisions, data protection officers are also needed to facilitate employee training and awareness programs, which ensure employees understand their role in safeguarding data.

Conclusion

This report has provided a comprehensive analysis of the similarities and differences between the Personal Data Protection Act (PDPA) and the General Data Protection Regulation (GDPR), with a focus on their definitions, scope, principles, and implications for organizations managing personal data. Both frameworks aim to safeguard personal data, but they do so with distinct approaches tailored to their jurisdictions.

The GDPR emphasizes individual rights, accountability, and detailed procedural requirements, making it highly comprehensive but resource-intensive for organizations. Its inclusion of rights such as data portability, objection to processing, and erasure reflects its strong emphasis on empowering data subjects. Conversely, the PDPA adopts a more practical approach, focusing on explicit consent, accountability, and flexibility to support businesses in Singapore. While it ensures fundamental protections, it does not match the depth or breadth of rights provided under the GDPR.

For organizations operating in multiple jurisdictions, compliance with both frameworks is essential to maintain trust, avoid penalties, and ensure robust data protection. This requires a nuanced understanding of their overlapping principles and divergent requirements. The challenges posed by cross-border data transfers, resource allocation for compliance, and the evolving nature of cybersecurity threats further highlight the need for proactive measures and alignment with these regulations.

In conclusion, understanding the nature of personal data and the frameworks that govern it is vital for organizations navigating today’s globalized and digitally interconnected environment. Both the PDPA and GDPR set the foundation for responsible data management, and their adoption not only ensures legal compliance but also builds stakeholder trust, enhances cybersecurity strategies, and promotes the ethical handling of personal information in an increasingly data-driven world.

Task Allocation and Personal Reflection

Task Allocation

Name	Tasks
Damien Hoi	Challenges in Data Protection
Russell Chin	Scope
Aung Kaung Chit	PDPA vs GDPR : Relation to Data Protection for Cyber Security Conclusion
Li Hao	Introduction Definition Accountability and Obligations Key Differences

Personal reflection

Damien:

While working on this project on “PDPA vs GDPR: Understanding the Nature of Personal Data”, I gained a deeper knowledge of data protection laws and realized how complex and difficult it is for organizations to navigate and use these different frameworks to fulfill what they need. I also understood that both PDPA and GDPR frameworks allowed me to understand that both aim to protect personal data, but have different approaches to doing so. Both frameworks have their pros and cons in helping organizations and individuals protect and safeguard their data online. GDPR offers individual control over personal data, which I realized gives individuals rights over their personal information. PDPA, on the other hand, offers more flexibility for businesses and organizations, particularly for business objectives. It mainly focuses on gaining consent and ensuring data retention, however, it does not provide as many rights as compared to what GDPR has. Furthermore, the roles of the Data Protection Officer (DPO) work differently in both of the frameworks. The GRPR requires their DPO to be independent and highly qualified, which I feel is really important in ensuring effective and reliable data protection. PDPA, they are more flexible and is allowed to have team-based DPO, which can also be an advantage in different situations where they can work together. In essence, this project has given me a better understanding of what data protection is and how it affects the real world. It also allows me to see that organizations must juggle between the protection of data and individual rights across different environments, which may be a constant challenge.

Li Hao:

Working on the report "PDPA vs GDPR: Understanding the Nature of Personal Data" provided valuable insights into the complexities of data protection laws and their role in today’s digital world. Comparing the Singapore PDPA and the EU GDPR highlighted how these frameworks address personal data protection with distinct priorities. The GDPR's emphasis on extensive individual rights, such as data portability and the right to be forgotten, contrasts with the PDPA's practical, business-friendly approach that focuses on consent and flexibility.

I particularly appreciated learning about the accountability obligations under both frameworks. While both require organizations to appoint Data Protection Officers (DPOs), the GDPR mandates independence for the role, whereas the PDPA allows a more adaptable, team-based setup. This difference reflects how regulations cater to varying operational needs. Additionally, the project emphasized the critical role of cybersecurity measures, like encryption and audits, in mitigating risks, alongside the importance of employee training to address human errors.

Exploring the challenges of cross-border data transfers was especially eye-opening. The GDPR’s strict mechanisms for ensuring data protection across jurisdictions contrast with the PDPA’s more adaptable approach, allowing businesses to customize safeguards. This illustrates the complexity organizations face in aligning compliance strategies globally.

Overall, this project enhanced my understanding of how data protection laws intersect with cybersecurity practices. It underscored the need for a balanced approach to compliance, where organizations protect personal data while achieving operational goals. This knowledge will be invaluable as I pursue a career in cybersecurity, helping to ensure data privacy and foster trust in digital systems.

Aung Kaung Chit:

In this assignment, I am responsible for “PDPA vs GDPR: Relation to Data Protection for Cyber Security” section, in which I had to consolidate all the understandings about how PDPA and GDPR facilitate safeguarding of personal data in various aspects. To achieve this, I undertook the following steps:

- Research and comparison where I explored the similarities and differences between PDPA (Personal Data Protection Act) and GDPR (General Data Protection Regulation) in terms of scope, enforcement, and data protection principles focusing on key aspects like privacy by design, data subject rights, and accountability to highlight their relevance to cybersecurity.
- Incorporation of real-world example such as the use of Data Protection Impact Assessments (DPIAs) to evaluate risks in deploying data-intensive systems like customer relationship management (CRM) platforms.
- Emphasis on cybersecurity practices that linked the frameworks to cybersecurity measures, such as encryption, pseudonymization, secure access controls, and regular audits, demonstrating their importance in protecting confidentiality, integrity, and availability.

Overall, this assignment is crucial to me as it provides the understanding and awareness of compliance in cyber security.

Russell

As I worked together with my teammates on this assignment on “GDPR vs PDPA”, I gained many valuable insights on the comparison of these 2 data protection laws. The process of researching on these 2 frameworks allowed me to gain a full understanding of their distinct definitions, approaches, scope, and challenges. Both frameworks share the principle of safeguarding personal data for living individuals. One of the key insights I developed is the importance of **personal scope** and **territorial scope** in determining who and where the regulations apply. For instance, for the personal scope, both PDPA and GDPR only protects living indivudual’s personal data, but the PDPA has some exceptions under certain circumstances. GDPR entirely excludes deceased individuals from its protection, in comparison to PDPA, which protects data for up to 10 years after death or excluding records that are over 100 years old. For an example of territorial scope, GDPR has comprehensive coverage of both public and private entities in the EU, and its extraterritorial reach ensure robust protection for EU residents' data globally. In comparison to PDPA, which excludes public agencies, and focuses on organizations that collect, use or disclose activities personal data in Singapore, whether or not the organisation is local or foreign, or even physically present in Singapore. Additionally, for Material Scope, GDPR’s differentiation of special categories of sensitive data and its inclusion of non-automated data processing as part of its scope reflect its meticulous and detailed approach. This ensures enhanced safeguards for highly sensitive data and leaves no gaps in coverage, even for physical records. PDPA, by contrast, adopts a more generalized approach, treating all types of personal data uniformly and it focuses on the collection, use, and disclosure of personal data in Singapore.This knowledge is extremely important for me as a Cybersecurity student. As I enter the workforce, it is of upmost importance that the job that I take, regardless of it being in the public sector like working for the Government, or working in a private sector job. It is crucial that the organisation complies with the relevant data protection laws, and that I do my part to ensure that the actions an organisation take would comply with the correct data protection frameworks which would help to ensure that the individuals’ personal data are well protected, and also to prevent the organisation from suffering damages from not complying with the applicable laws.

References

SNIA. *What is Data Protection?* [online]. Available from: https://www.snia.org/education/what-is-data-protection [Accessed: 20 November 2024]

Personal Data Protection Commission (PDPC) Singapore, 2021. *GUIDE TO DATA PROTECTION IMPACT ASSESSMENTS* [online]. Available form: https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/other-guides/dpia/guide-to-data-protection-impact-assessments-14-sep-2021.pdf [Accessed: 22 November 2024]

Pecb (no date) Data protection challenges. https://pecb.com/article/data-protection-challenges. [Accessed: 22 November 2024]

De Vente, P. (2024) The challenges of data protection and ways organizations can address them. https://blog.quest.com/the-challenges-of-data-protection-and-ways-organizations-can-address-them/. [Accessed: 22 November 2024]

McCormick, J. (2024) 6 data privacy challenges and how to fix them. https://www.techtarget.com/searchdatamanagement/feature/Top-3-data-privacy-challenges-and-how-to-address-them. [Accessed: 22 November 2024]

Standard Contractual Clauses (SCC) (2021). https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en. [Accessed: 22 November 2024]

River, R. (2024) 4 Key challenges for data protection and privacy in 2024 and beyond. https://redriver.com/security/data-protection-and-privacy. [Accessed: 22 November 2024]

The European Union (EU) General Data Protection Regulation (GDPR) (2022). https://www.hrpo.pitt.edu/european-union-eu-general-data-protection-regulation-gdpr#:~:text=The%20General%20Data%20Protection%20Regulation,of%20individuals%20in%20the%20EEA.